DISCRETE GEOMETRY: LATTICE POLYTOPES

CARSTEN LANGE

1. Introduction

These lectures on discrete geometry combine various areas of mathematics. In particular, we shall study a close relationship between geometry and algebra. Polytopes are geometric objects that draw attention of mathematicians and non-mathematians for more than 2000 years: Egyptian pyramids (aka pyramid over a square) as well as platonic and archimedean solids are ancient examples that fascinate humans over and over again. Polytopes are also the fundamental building block of linear optimization theory which was applied for the first time by the US army during the Berlin air lift to make good use of scarce resources for transportation. The related linear programs were solved by hand and, due to the availability of computers, more complicated models have been used by private companies (starting with oil companies in the 1950s). Lattices are algebraic objects but their prime application (crystallography) already intertwines algebra and geometry.

We denote finite dimensional $\mathbb{R}$-vector spaces by V, V_i, V', etc, while we denote by $\mathbb{R}^d$ the euclidean $\mathbb{R}$-vector space of dimension d endowed with the euclidean norm $\|v\| = \sum_{i\in[d]} \lambda_i^2$ where $[d] = \{1, 2, \ldots, d\}$, $v = \sum_{i\in[d]} \lambda_i e_i$ and $\{e_i\}_{i\in[d]}$ is the standard (orthonormal) basis for $\mathbb{R}^d$. Recall that the euclidean distance in $\mathbb{R}^d$ between two points $x, y \in \mathbb{R}^d$ is defined as $\mathsf{dist}(x, y) := \|x - y\|$ while the distance between $x \in \mathbb{R}^d$ and $S \subseteq \mathbb{R}^d$ is $\mathsf{dist}(x, S) := \inf_{s\in S} \mathsf{dist}(x, s)$. Similarly, the distance between $S, T \subseteq \mathbb{R}^d$ is $\mathsf{dist}(S, T) := \inf_{s\in S,\ t\in T} \mathsf{dist}(s, t)$.

Recall from linear algebra that there are two natural nontrivial volume functions on a subspace V of $\mathbb{R}^d$ if a basis $\mathcal{B} = \{v_i\}_{i\in[d']}$ is given for V. First, we obtain a volume $\mathsf{vol}_{\mathcal{B}}$ on V by the auxiliary euclidean structure on V where $\mathcal{B}$ is forced to be an orthonormal basis, and, second, the volume $\mathsf{vol}_{\mathbb{R}^d}$ on $\mathbb{R}^d$ induces a volume on V by choosing some basis for V that extends to an orthonormal basis for $\mathbb{R}^d$. We abuse notion and denote the latter volume also by $\mathsf{vol}_{\mathbb{R}^d}$. For measurable subsets $K \subseteq V$, both volumes are clearly invariant with respect to V-translations. The closed and half-open parallelepiped of a basis $\mathcal{B}$ for $V \subseteq \mathbb{R}^d$ are $\overline{\Pi}_{\mathcal{B}} := \left\{ \sum_{i\in[d]} \lambda_i v_i \;\middle|\; 0 \le \lambda_i \le 1 \text{ for all } i \in [d] \right\}$ and $\Pi_{\mathcal{B}} = \left\{ v = \sum_{i\in[d]} \lambda_i v_i \;\middle|\; 0 \le \lambda_i < 1 \text{ for all } i \in [d] \right\}$.

1.1. Polytopes.

There are two equivalent definitions of a polytope P. One is in terms of points (which is a superset of the vertices of P) while the other is in terms of linear inequalities (linear half-spaces).

Definition 1.1 (V-polytope)**.**
Any finite set of points $\{p_1, \ldots, p_n\} \subset R^d$ defines a V-polytope:

$$P_V := \mathsf{conv}\{p_1, \ldots, p_n\}.$$

Definition 1.2 (H-polytope)**.**
Any matrix $A \in \mathbb{R}^{n\times d}$ and any matrix $b \in \mathbb{R}^n$ define an H-polyhedron:

$$P_H := \left\{ x \in \mathbb{R}^d \;\middle|\; Ax \le b \right\}.$$

An H-polytope P is a bounded H-polyhedron.

The main theorem of polytope theory states that the notions of V-polytopes and H-polytopes coincide. Thus we do not distinguish between H- and V-polytopes and speak of polytopes only.

Any polytope P spans an affine subspace $\mathsf{aff}(P) \subseteq \mathbb{R}^d$ and the dimension of this this affine subspace defines the dimension of P: $\dim(P) := \dim(\mathsf{aff}(P))$. Clearly, we have $\dim(P) \leq d$.

Polytopes allow many distinct notions of equivalence. Examples of geometric equivalences for polytopes are induced by various classes of transformations. For example, the class of transformations may only consist of the identity $\mathsf{Id} : \mathbb{R}^d \to \mathbb{R}^d$, of all rotations, of all elements of $SO(V)$ or $O(V)$, of all euclidean transformations, of all affine transformations or of all projective transformations. These choices clearly yield distinct equivalence classes. A combinatorial equivalence for polytopes is defined as follows. For a polytope P, the set $\mathcal{F}(P)$ of all faces of P is partially ordered by inclusion. We call two polytopes P and P' combinatorially equivalent if and only if $\mathcal{F}(P)$ and $\mathcal{F}(P')$ are isomorphic posets (=**p**artially **o**rdered **sets**). The poset $\mathcal{F}(P)$ of a polytope P is also known as the face lattice of P — be aware that here 'lattice' refers to an order theoretic lattice and not to a geometric lattices as defined in Section 1.2.

1.2. **Lattices.**

Let V be a euclidean vector space with norm $\| \ \|_V$, $x \in V$ and $\epsilon > 0$. The ball of radius ϵ centered at x is $B_\epsilon(x) := \{v \in V \ \mid \|v - x\|_V \leq \epsilon\}$.

Definition 1.3 (lattice)**.**
Let V be a euclidean vector space. A lattice $\Lambda \subset V$ is an additive subgroup of V such that for every $x \in \Lambda$ there exists $\epsilon > 0$ such that $B_\epsilon(x) \cap \Lambda = \{x\}$.

Recall from linear algebra that an additive subgroup $G \subseteq V$ is characterized by the following three properties: (i) $0 \in G$; (ii) $x + y \in G$ for all $x, y \in G$ and (iii) $-x \in G$ for all $x \in G$.

Definition 1.4 (lattice generated by $\mathcal{B} \subset V$)**.**
The lattice $\Lambda(\mathcal{B})$ generated by a linear independent set $\mathcal{B} = \{v_1, \ldots, v_d\} \subset V$ is

$$\Lambda(\mathcal{B}) := \left\{ \textstyle\sum_{i \in [d]} \lambda_i v_i \ \middle| \ \lambda_i \in \mathbb{Z} \text{ for all } i \in [d] \right\}.$$

The set $\mathcal{B}$ is called lattice basis for $\Lambda(\mathcal{B})$.

The main theorem of lattice theory states that every lattice according to Definition 1.3 can be described as a lattice according to Definiton 1.4. In particular, the rank $\mathsf{rk}(\Lambda)$ of a lattice $\Lambda \subset V$, defined as $\dim(\mathsf{span}_{\mathbb{R}}(\Lambda))$, coincides with the cardinality of any lattice basis for Λ.

Definition 1.5 (lattice homomorphisms)**.**
A lattice homomorphism is a map $f : \Lambda \to \Lambda'$ such that there exists a linear map $F : \mathsf{span}_{\mathbb{R}}(\Lambda) \to \mathsf{span}_{\mathbb{R}}(\Lambda')$ that restricts to f. Following standard terminology from algebra, we call f a lattice iso-, epi- or monomorphism if and only if f is bijective, surjective or injective. A lattice automorphism is a lattice isomorphism $f : \Lambda \to \Lambda$.

Two lattices are clearly isomorphic if and only if their ranks are equal. Moreover, any lattice Λ is lattice isomorphic to $\mathbb{Z}^{\mathsf{rk}(\Lambda)}$. The notion of equivalent lattices is refined by taking additional geometric information into account. As it turns out, the volume of the parallelepiped of a lattice basis does not depend on the chosen lattice basis. Two lattices $\Lambda \subset \mathbb{R}^d$ and $\Lambda' \subset \mathbb{R}^{d'}$ are called unimodular equivalent if and only if $\mathsf{rk}(\Lambda) = \mathsf{rk}(\Lambda')$ and $\mathsf{vol}_{\mathbb{R}^d}(\Pi_{\mathcal{B}}) = \mathsf{vol}_{\mathbb{R}^{d'}}(\Pi_{\mathcal{B}'})$ where $\mathcal{B} \subset \Lambda$ and $\mathcal{B}' \subset \Lambda'$ are lattice bases. Moreover, a lattice $\Lambda \subset \mathbb{R}^d$ is a unimodular lattice if and only if $\mathsf{vol}_{\mathbb{R}^d}(\Pi_{\mathcal{B}'}) = 1$.

Most of the time, it suffices if we restrict to lattices Λ of rank r in $\mathbb{R}^d$, that is if $\Lambda = \mathbb{Z}^r \subset \mathbb{R}^d$.

1.3. **Lattice Polytopes.**

Definition 1.6 (lattice polytope)**.**
Let $\Lambda \subset V$ be a lattice and $\{p_1, \ldots, p_n\} \subset \Lambda$ a finite set. Then $\mathsf{conv}\{p_1, \ldots, p_n\}$ is a lattice polytope.

The extra condition $\{p_1, \ldots, p_n\} \subset \Lambda$ that turns an arbitrary polytope into a lattice polytope has far reaching consequences. For those readers who know about linear optimization theory, we point out that lattice polytopes relate to integer and combinatorial optimization. For example, we may only be interested in integral solutions of a linear programme where we aim for optimal $\mathbb{Z}^d$-lattice points of our problem. To find such a solution can be difficult.

1.4. **Examples.**
A basic theme of these lectures is that we try to relate properties of polytopes (such as their 'form' or 'volume') to lattice properties (such as the number of lattice points contained by a lattice polytope). We now give a number of examples.

Example 1: Pick's formula
Let P be a lattice polygon, that is, P is a lattice polytope for $\Lambda = \mathbb{Z}^2 \subset \mathbb{R}^2$ with $\dim(P) = 2$. Moreover, denote the number of interior lattice points of P by $I(P)$ and the number of lattice points contained in the boundary of P by $B(P)$. Then Pick's formula relates the numbers $I(P)$ and $B(P)$ in a very nice and extremely simple way to the area $\mathsf{vol}_{\mathbb{R}^2}(P)$ of P:

$$\mathsf{vol}_{\mathbb{R}^2}(P) = I(P) + \frac{1}{2}B(P) - 1.$$

To prove Pick's formula, we proceed in two steps.

1) If the boundary ∂P of P contains at least four lattice points as vertices then we can use two vertices to dissect P into two lattice polygons P_1 and P_2 with fewer lattice points as vertices. Let S be the line segment contained by P_1 and P_2 and ℓ the number of lattice points of S. We clearly have the following three identities:

$$\begin{aligned} \mathsf{vol}_{\mathbb{R}^2}(P) &= \mathsf{vol}_{\mathbb{R}^2}(P_1) + \mathsf{vol}_{\mathbb{R}^2}(P_2) \\ I(P) &= I(P_1) + I(P_2) + \ell - 2 \\ B(P) &= B(P_1) + B(P_2) - 2\ell + 2. \end{aligned}$$

   These identities imply

$$I(P) + \tfrac{1}{2}B(P) - 1 = \big(I(P_1) + \tfrac{1}{2}B(P_1) - 1\big) + \big(I(P_2) + \tfrac{1}{2}B(P_2) - 1\big)$$

   and we conclude that Pick's formula is valid if it is valid for P_1 and P_2.

2) Any lattice polygon P with at least four lattice points as vertices can be dissected into to two lattice polygons with fewer vertices by using two vertices of P. Moreover, this is not possible if P has three lattice points as vertices. As a consequence, it suffices to prove Pick's formula for lattice polygons with precisely three vertices, that is, for arbitrary lattice triangles. This is not difficult and remains an exercise.

Pick's formula has the following two pleasant consequences

Corollary 1.7.
The area of every lattice triangle in $\mathbb{R}^2$ containing precisely three lattice points equals $\frac{1}{2}$.

Consider a lattice triangle T in $\mathbb{R}^2$ with vertices v_1, v_2 and v_3 that contains precisely three lattice points. The vectors $v_1 - v_2$ and $v_1 - v_3$ generate a lattice Λ and T is precisely one half of the parallelepiped spanned by these vectors. Clearly, the lattice Λ is unimodular by Corollary 1.7. For that reason, we also refer to T as unimodular triangle.

Corollary 1.8.
Every lattice polygon in $\mathbb{R}^2$ can be dissected into unimodular triangles.

Example 2: Scott's theorem
As we continue to consider lattice polygons, we continue to use the notation of Example 1. This second example provides an upper bound (in terms of $I(P)$) for the volume $\mathsf{vol}_{\mathbb{R}^d}(P)$ of a lattice polytope P that has at least one interior lattice point. We certainly need $I(P) \geq 1$ for such a bound. Moreover, such a bound does not exist if we consider (arbitrary) convex polygons instead of convex lattice polygons. A family of polytopes with precisely one interior lattice point of arbitrary

volume are easily constructed. Results that relate the number of lattice points of a convex body to its shape or to geometric invariants are subsumed under the name 'Geometry of numbers'.

Theorem 1.9.
If $P \subset \mathbb{R}^2$ is a lattice polygon with $I(P) \geq 1$ then one of the following statements is true:
i) $\mathsf{vol}_{\mathbb{R}^2}(P) \leq 2\,(I(P)+1)$.
ii) $P = 3 \cdot \mathsf{conv}\{0, e_1, e_2\}$.

Remark 1.10.
a) For $k > 0$, the k^{th}-dilate kP of a lattice polytope $P = \mathsf{conv}\{v_1, \ldots, v_r\} \subset \mathbb{R}^d$ is defined as $\mathsf{conv}\{kv_1, \ldots, kv_r\}$. Geometrically, the k^{th}-dilate kP can be constructed as follows. Realize P in $\mathbb{R}^{d_1} = \mathbb{R}^d \times \mathbb{R}$ at height $x_{d+1} = 1$, consider the rays ρ_i emanating from the origin through v_i and define $\tilde{v}_i$ as the unique point on ρ_i such that $x_{d+1} = k$. Then kP is $\mathsf{conv}\{\tilde{v}_1, \ldots, \tilde{v}_r\}$.
b) $P = 3 \cdot \mathsf{conv}\{0, e_1, e_2\}$ satisfies $B(P) = 9$, $I(P) = 1$ and $\mathsf{vol}_{\mathbb{R}^2}(P) = \frac{9}{2} > 2\,(I(P)+1)$, so it is impossible that both statements hold simultaneously .

Example 3: Knapsack problems
The goal of Knapsack problems is to fill a knapsack of a certain capacity C with certain products. There are k products to choose from and it is assumed that product i has an assigned volume v_i and price p_i. Notice that the model only concerns the volume measure, the shape of the objects is not fixed. Moreover, it is not possible to split products into smaller quantities. The following two knapsack problems are common:

i) 0/1-knapsack
Fill the knapsack such that the value of chosen products is maximized. Each product can be chosen or discarded, no multiples are allowed (if we assume that the goods are distinct):
$$\begin{gathered} \max\ x_1p_1 + \ldots + x_kp_k \\ s.t.\ x_1v_1 + \ldots + x_kv_k \leq C \\ x_i \in \{0,1\} \text{ for } i \in [k] \end{gathered}$$

ii) bounded knapsack
Fill the knapsack such that the value of chosen products is maximized. Each product can be chosen or discarded, multiples are allowed:
$$\begin{gathered} \max\ x_1p_1 + \ldots + x_kp_k \\ s.t.\ x_1v_1 + \ldots + x_kv_k \leq C \\ x_i \in \mathbb{N}_0 \text{ for } i \in [k] \end{gathered}$$

The relation to polytopes and lattice points is obvious: consider the polytope $P \subset \mathbb{R}^k$ defined by $x_1v_1 + \ldots + x_kv_k \leq C$ and $x_i \geq 0$ for $i \in [k]$. This polytope is not necessarily a lattice polytope but we find the optimal solutions among $P \cap \{0;1\}^k$ and $P \cap (\mathbb{N}_0)^k$ which are sets of lattice points.

Example 4: Coin change problem
A variation of the knapsack problems mentioned in Example 2 is
$$\begin{gathered} x_1p_1 + \ldots + x_kp_k = V \\ s.t.\ x_1v_1 + \ldots + x_kv_k = C \\ x_i \in \mathbb{N}_0 \text{ for } i \in [k]. \end{gathered}$$
This problem can be rephrased as a coin change problem: suppose our currency has k distinct coins and that we are interested in the number of distinct ways to put precisely C coins of value V into our wallet. For example, if our currency is US$ then there are four coins — a penny ($p_1 = 1$ cent), a nickel ($p_2 = 5$ cent), a dime ($p_3 = 10$ cent) and a quarter ($p_4 = 25$ cent) — and there are precisely four ways to fill our wallet with 10 coins worth 1 dollar. The four solutions are:
$$\begin{aligned} 100 &= 5 \cdot 1 + 0 \cdot 5 + 2 \cdot 10 + 3 \cdot 25 \\ &= 0 \cdot 1 + 6 \cdot 5 + 2 \cdot 10 + 2 \cdot 25 \\ &= 0 \cdot 1 + 3 \cdot 5 + 6 \cdot 10 + 1 \cdot 25 \\ &= 0 \cdot 1 + 0 \cdot 5 + 10 \cdot 10 + 0 \cdot 25. \end{aligned}$$

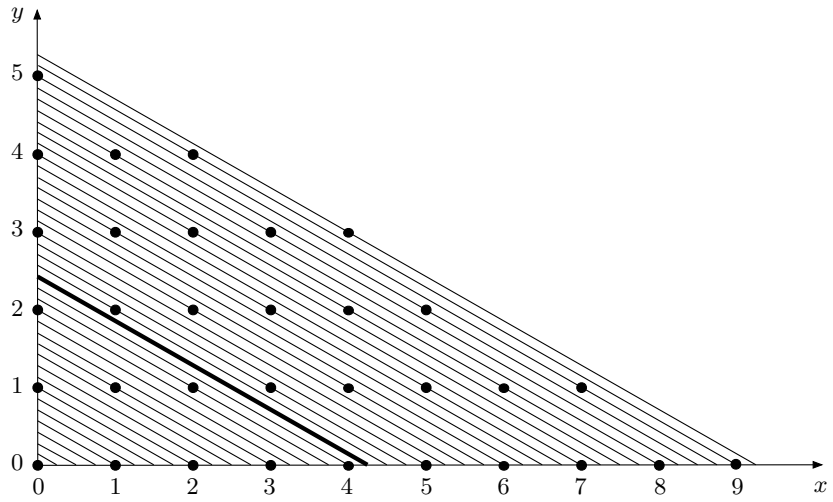

FIGURE 1. The 2-dimensional Frobenius problem for $a_1 = 4$ and $a_2 = 7$. The dilates $P_k = kP_1$ of P_1 are shown for $k \in [37]$. The thick line segment is P_{17} and does not contain any lattice point of $\Lambda = \mathbb{Z}^2$.

From a polytope perspective, the polytope

$$P := \left\{ x \in \mathbb{R}^4 \;\middle|\; \begin{smallmatrix} x_1+5x_2+10x_3+25x_4=100 \\ x_1+x_2+x_3+x_4=10 \\ x_i \geq 0 \text{ for } i \in [k] \end{smallmatrix} \right\}$$

contains precisely four lattice points: $|P \cap \mathbb{Z}^4| = 4$. This is a rather small and simple example and can be worked out by hand. But we need a more systematic way to determine the 182 ways to have 100 coins worth 10 dollar and the 15,876 ways to have 1000 coins worth 100 dollar.

Example 5: coin exchange problem of Frobenius
Suppose that our currency does not use pennies, nickels, dimes and quarters but the only existing denominations of coins are 4 and 7 cent. This system has an obvious flaw: we are not able to change 1 cent or 5 cent or 10 cent.

More general, the Frobenius coin exchange problem (also known as the *linear Diophantine problem of Frobenius*) is the following problem. Suppose a currency has k distinct coins of denomination $a_i \in \mathbb{N}$, $i \in [k]$, without any (nontrivial) common factor, that is, $\gcd(a_1, \ldots, a_k) = 1$. What is the largest amount that cannot be changed using these coins? This number is known as Frobenius number (of course, it has to be checked that this number is well-defined.

How relates the Frobenius number to polytopes and lattice points? For $n \in [\mathbb{N}]$, consider

$$P_n := \left\{ x \in \mathbb{R}^d \;\middle|\; \begin{smallmatrix} x_1a_1+\ldots+x_ka_k=n \\ x_i \geq 0 \text{ for } i \in [k] \end{smallmatrix} \right\}.$$

Then the restricted partition function[1] is $p(n) := |\mathbb{Z}^k \cap P_n|$ and the Frobenius number is the largest integer n such that $p(n) = 0$. As the polytope P_n is the n^{th} dilate of P_1, we can rephrase the problem and ask for the largest n such that the n^{th} dilate of P_1 does not contain any lattice point of $\Lambda = \mathbb{Z}^d$.

We return to our example with $d = 2$, $a_1 = 4$ and $a_2 = 7$. Then P_1 is the line segment in the first quadrant of $\mathbb{R}^2$ with end points $(\frac{1}{4}, 0)$ and $(0, \frac{1}{7})$. The first 37 dilates of P_1 are illustrated in Figure 1.4. The figure suggests that P_{17} is the largest dilate P_n of P_1 that contains no lattice point of $\mathbb{Z}^2$ – at least we see that P_k contains a lattice point for $18 \leq k \leq 37$.

[1]Recall that a partition of $n \in \mathbb{N}$ is a multiset of integers $\{n_1, \ldots, n_r\}$ of positive integers such that $n = \sum_{i \in [r]} n_i$. A restricted partition is a partition with $n_i \in M$ for some $M \subseteq \mathbb{N}$. The function $p(n)$ provides the number of restricted partitions of n with $M = \{a_1, \ldots, a_k\}$.

Using generating functions, the 2-dimensional Frobenius problem for positive integers a_1 and a_2 with $\gcd(a_1, a_2) = 1$ can be solved explicitly. In this case, the Frobenius number equals $a_1a_2 - a_1 - a_2$. In fact, we obtain $4 \cdot 7 - 4 - 7 = 17$ as conjectured!

Example 6: Contingency tables
The following table is a simplified version of a table published by Statistische Landesamt Berlin in 2005 and provides the number of academic degrees — diploma, PhD, teacher — awarded by three universities in Berlin — Humboldt Universität (HU), Freie Universität (FU) and Technische Universität (TU). Assuming uniform distribution, we wonder how likely this distribution of entries actually is. In other words, how many tables with the same margin sums — the totals per column and row for the universities and awarded degrees — are there?

	diploma	PhD	teacher	
HU	920	441	373	1734
FU	1989	1444	299	3731
TU	1868	421	115	2404
	4777	2306	787	

This problem is solved by counting the $714,574,663,432$ lattice points of the polytope

$$P := \left\{ x \in \mathbb{R}^9 \;\middle|\; \begin{array}{ll} x_1 + x_2 + x_3 = 1734, & x_1 + x_4 + x_7 = 4777, \\ x_4 + x_5 + x_6 = 3731, & x_2 + x_5 + x_8 = 2306, \text{ and } x_i \geq 0 \text{ for } i \in [9] \\ x_7 + x_8 + x_9 = 2404, & x_3 + x_6 + x_7 = 787, \end{array} \right\}.$$

We shall also discuss algorithmic aspects of lattice point counting for polytopes.

Example 7: Toric varieties
The classical way to define an algebraic variety is to consider the set of all common zeroes of a set of polynomials in n complex variables. If we consider only one polynomial of degree d in one variable, then the corresponding algebraic variety consists of at most d isolated points in the complex plane. But things get much more complicated if one considers polynomials in more than one variable or if one considers more than polynomial. Linear algebra tells us how to answer this question if the polynomials are of degree one and for two polynomials P and Q in one variable, the resultant helps to decide whether P and Q have common zeroes not.

Toric varieties are a special class of algebraic varieties. A toric variety T has the special property that T contains an algebraic torus $(\mathbb{C}^*)^n = (\mathbb{C} \setminus \{0\})^n$ for some $n \in \mathbb{N}$ as well as an action of $(\mathbb{C}^*)^n$ on itself that extends to an action of the torus on T. Toric varieties can can be encoded by a fan Σ and the fundamental theorem of toric varieties states that every normal toric variety associated to a fan Σ in $\mathbb{R}^n$ is projective if and only if Σ is the normal fan of a lattice polytope in $\mathbb{R}^n$. Even without understanding the details, one might see that this characterization can be very powerful. Properties of a toric variety can be studied in terms of properties of lattice polytopes and vice versa. We come back to toric varieties later and explain the meaning of the above statements in more detail (with examples) after we reviewed the basics of fans, cones and polytopes.

2. Basics on lattices

In this section, we prove the two fundamental properties of lattices mentioned in the introduction: every lattice has a lattice basis and the volume of a parallelepiped determined by a lattice basis is actually independent of the chosen basis.

2.1. **Existence of a lattice basis.**

To prove the existence of a lattice basis of a lattice $\Lambda \subset \mathbb{R}^d$, we first prove the auxiliary result that for every proper subspace $V \subset \mathsf{span}_{\mathbb{R}}(\Lambda)$ there exists a lattice point $x \in \Lambda \setminus V$ such that $\mathsf{dist}(x, V) = \mathsf{dist}(V, \Lambda \setminus V)$.

Lemma 2.1.
Let $\Lambda \subset \mathbb{R}^d$ be a lattice, $b_1, \dots b_\ell \in \Lambda$ linearly independent with $\ell < \mathsf{rk}(\Lambda)$ and $V := \mathsf{span}_{\mathbb{R}}\{b_1, \dots b_\ell\}$. Then there exist $x \in \Lambda \setminus V$ and $v \in V$ such that

$$\mathsf{dist}(x, v) \leq \mathsf{dist}(\widetilde{x}, \widetilde{v}) \qquad \text{for all } \widetilde{x} \in \Lambda \setminus V \text{ and } \widetilde{v} \in V.$$

Proof. The set $\mathcal{B} := \{b_1, \dots b_\ell\}$ generates the lattice $\Lambda_{\mathcal{B}} \subset \Lambda$ and yields the closed parallelepiped $\overline{\Pi}_{\mathcal{B}}$ which is compact. We first show that there is a $x \in \Lambda \setminus V$ that achieves $\mathsf{dist}(\overline{\Pi}_{\mathcal{B}}, \Lambda \setminus V)$. To this direction, choose $w \in \Lambda \setminus V$ and set $\rho := \mathsf{dist}(w, \overline{\Pi}_{\mathcal{B}})$. Moreover, define the ρ-neighbourhood of $\overline{\Pi}_{\mathcal{B}}$ via $\overline{\Pi}_{\mathcal{B},\rho} := \left\{x \in \mathbb{R}^d \;\middle|\; \mathsf{dist}(x, \overline{\Pi}_{\mathcal{B}}) \leq \rho\right\}$. Since $\overline{\Pi}_{\mathcal{B},\rho}$ is compact and since Λ is discrete, the intersection $\overline{\Pi}_{\mathcal{B},\rho} \cap \Lambda$ is finite. Moreover, $\left(\overline{\Pi}_{\mathcal{B},\rho} \cap \Lambda\right) \setminus V \neq \varnothing$. Therefore, we find a point $x \in \left(\overline{\Pi}_{\mathcal{B},\rho} \cap \Lambda\right) \setminus V$ that achieves the distance to $\overline{\Pi}_{\mathcal{B}}$:

$$\mathsf{dist}(x, \overline{\Pi}_{\mathcal{B}}) \leq \mathsf{dist}(w, \overline{\Pi}_{\mathcal{B}}) \qquad \text{for all } w \in \left(\overline{\Pi}_{\mathcal{B},\rho} \cap \Lambda\right) \setminus V.$$

We also find a point $v \in \overline{\Pi}_{\mathcal{B}}$ that achieves the distance between x and $\overline{\Pi}_{\mathcal{B}}$, that is,

$$\mathsf{dist}(x, v) = \mathsf{dist}(x, \overline{\Pi}_{\mathcal{B}}).$$

We now show that our choices for x and v fulfill

$$\mathsf{dist}(x, v) \leq \mathsf{dist}(\widetilde{x}, \widetilde{v}) \qquad \text{for all } \widetilde{x} \in \Lambda \setminus V \text{ and } \widetilde{v} \in V.$$

Choose $\widetilde{x} \in \Lambda \setminus V$ and $\widetilde{v} = \sum_{i \in [\ell]} \lambda_i b_i \in V$. As $z := \sum_{i \in [\ell]} \lfloor \lambda_i \rfloor b_i \in \Lambda$ we have

$$\widetilde{x} - z \in \Lambda \setminus V, \text{ and} \qquad \widetilde{v} - z := \sum_{i \in [\ell]} (\lambda_i - \lfloor \lambda_i \rfloor)\, b_i \in \overline{\Pi}_{\mathcal{B}}.$$

This implies

$$\mathsf{dist}(x, v) = \mathsf{dist}(x, \overline{\Pi}_{\mathcal{B}}) \leq \mathsf{dist}(\widetilde{x} - z, \overline{\Pi}_{\mathcal{B}} \leq \mathsf{dist}(\widetilde{x} - z, \widetilde{v} - z) = \mathsf{dist}(\widetilde{x}, \widetilde{v})$$

which finishes the proof of the lemma. □

Theorem 2.2.
Let $\Lambda \subset \mathbb{R}^d$ be a lattice and $\{b_1, \dots, b_k\}$ be a basis of $\mathsf{span}_{\mathbb{R}}(\Lambda)$. Consider the nested sequence of subspaces $L_\ell \subset \mathsf{span}_{\mathbb{R}}(\Lambda)$ defined by $L_\ell := \mathsf{span}_{\mathbb{R}}\{b_1, \dots, b_\ell\}$ for $0 \leq \ell \leq k$ and let u_ℓ be a lattice point in $L_\ell \setminus L_{\ell-1}$ closest to $L_{\ell-1}$. Then $\{u_1, \dots, u_k\}$ is a lattice basis of Λ.

Proof. We first remark that Lemma 2.1 implies the existence of the vectors u_i for $i \in [k]$. Notice that $\Lambda_\ell := \Lambda \cap L_\ell$ for $\ell \in [k]$ is a lattice in $\mathbb{R}^\ell$. We proceed by induction on ℓ to show that $\{u_1, \dots, u_\ell\}$ is a lattice basis of Λ_ℓ.

First, notice that $L_0 = \{0\}$, so $u_1 = \lambda b_1$ for some $\lambda \in \mathbb{R} \setminus \{0\}$ and we have to show that $\{u_1\}$ is a lattice basis of Λ_1, that is, for every $v \in \Lambda_1$ there is a $\nu \in \mathbb{Z}$ such that $v = \nu u_1$. As $v = \mu b_1$ for some $\mu \in \mathbb{R}$, it suffices to show that $\nu := \frac{\mu}{\lambda} \in \mathbb{Z}$. If $\nu \notin \mathbb{Z}$ then $0 < \nu - \lfloor \nu \rfloor < 1$. In particular, $\widetilde{u}_1 := v - \lfloor \nu \rfloor u_1$ satisfies

$$\widetilde{u}_1 \in \Lambda_1 \setminus \{0\} \qquad \text{and} \qquad \widetilde{u}_1 = (\nu - \lfloor \nu \rfloor)\, u_1.$$

This clearly implies that $\widetilde{u}_1$ is closer to $\Lambda_1 \setminus \Lambda_0$ than u_1 which contradicts the choice of u_1. This shows $\nu \in \mathbb{Z}$ and $\{u_1\}$ is a lattice basis of Λ_1.

The inductive step is proven similarly. For $1 < \ell \leq k$, we know that $\{u_1, \dots, u_{\ell-1}\}$ is a lattice basis of $\Lambda_{\ell-1}$ and that $u_\ell = \sum_{i \in [\ell]} \lambda_i b_i$ with $\lambda_i \in \mathbb{R}$ for $i \in [\ell - 1]$ and $\lambda_\ell \in \mathbb{R}^*$. We have to

show that $\{u_1, \dots, u_\ell\}$ is a lattice basis of Λ_ℓ, that is, for every $v \in \Lambda_\ell$ there are $\nu_i \in \mathbb{Z}$ for $i \in [\ell]$ such that $v = \sum_{i\in[\ell]} \nu_i u_i$. If $v \in \Lambda_\ell$ then $v = \sum_{i\in[\ell]} \mu_i b_i$ with $\mu_i \in \mathbb{R}$ and we first claim that $\nu_\ell := \frac{\mu_\ell}{\lambda_\ell} \in \mathbb{Z}$. If $\nu_\ell \notin \mathbb{Z}$ then $0 < \nu_\ell - \lfloor \nu_\ell \rfloor < 1$. In particular, $\widetilde{u}_\ell := v - \lfloor \nu_\ell \rfloor u_\ell$ satisfies

$$\widetilde{u}_\ell \in \Lambda_\ell \setminus \Lambda_{\ell-1} \qquad \text{and} \qquad \widetilde{u}_\ell = \sum_{i\in[\ell-1]} (\mu_i - \lfloor \nu_\ell \rfloor \lambda_i)\, b_i + (\nu_\ell - \lfloor \nu_\ell \rfloor)\, \lambda_\ell b_\ell.$$

This implies that $\widetilde{u}_\ell$ is closer to $\Lambda_\ell \setminus \Lambda_{\ell-1}$ than u_ℓ which contradicts the choice of u_ℓ. This proves $\nu_\ell \in \mathbb{Z}$. But this implies $v - \nu_\ell u_\ell \in \Lambda_{\ell-1}$ and, by the induction hypothesis, we conclude that $v = \sum_{i\in[\ell]} \nu_i u_i$ where all $\nu_i \in \mathbb{Z}$. □

Corollary 2.3.
Every lattice $\Lambda \subset \mathbb{R}^d$ with $\mathsf{rk}(\Lambda) > 0$ has a lattice basis.

Definition 2.4 (fundamental parallelepiped)**.**
Let $\Lambda \subset \mathbb{R}^d$ be a lattice and $\mathcal{B} = \{b_1, \dots b_\ell\}$ a lattice basis for Λ. The half-open parallelepiped $\Pi_\mathcal{B}$ is the fundamental parallelepiped of the lattice basis $\mathcal{B}$ of Λ and a fundamental parallelepiped of the lattice Λ.

To emphasise the fact that the choice of a fundamental parallelepiped Π_Λ of a lattice $\Lambda \subset \mathbb{R}^d$ implicitly determines a basis $\mathcal{B}$ that generates Λ, we abuse notation and denote a fundamental parallelepiped of Λ as well as the fundamental parallelepiped of Λ by $\Pi_\mathcal{B}$.

We end this subsection by the following useful observation for any lattice $\Lambda \subset \mathbb{R}^d$. Translates of a fundamental parallelepiped $\Pi_\mathcal{B}$ of λ by lattice vectors tile $\mathsf{span}_\mathbb{R}(\Lambda)$.

Lemma 2.5.
Let $\Pi_\mathcal{B}$ be a fundamental parallelepiped of a lattice $\Lambda \subset \mathbb{R}^d$ and $x \in \mathbb{R}^d$. Then there exist uniquely determined $v \in \Lambda$ and $y \in \Pi_\mathcal{B}$ such that $x = v + y$.

Proof. Let $\Pi_\mathcal{B}$ be a fundamental parallelepiped of the lattice basis $\mathcal{B} = \{b_1, \dots b_\ell\}$ of $\Lambda \subset \mathbb{R}^d$. Then every $x \in \mathsf{span}_\mathbb{R}(\Lambda)$ has coordinates λ_i with respect to $\mathcal{B}$, that is, $x = \sum_{i\in[\ell]} \lambda_i b_i$. If we set $v := \sum_{i\in[\ell]} \lfloor \lambda_i \rfloor b_i$ and $y := \sum_{i\in[\ell]} (\lambda_i - \lfloor \lambda_i \rfloor)\, b_i$ then $v \in \Lambda$, $y \in \Pi_\mathcal{B}$ and $x = v + y$. This settles existence of the decomposition.

We now show that the decomposition is unique and suppose that $x = v + y = \widetilde{v} + \widetilde{y}$ where $v, \widetilde{v} \in \Lambda$ and $y, \widetilde{y} \in \Pi_\mathcal{B}$. We expand y and $\widetilde{y}$ with respect to $\mathcal{B}$ as

$$y = \sum_{i\in[\ell]} \lambda_i b_i \qquad \text{and} \qquad \widetilde{y} = \sum_{i\in[\ell]} \widetilde{\lambda}_i b_i$$

for $0 \le \lambda_i, \widetilde{\lambda}_i < 1$ and $i \in [\ell]$. Then

$$v - \widetilde{v} = \widetilde{y} - y = \sum_{i\in[\ell]} \left(\widetilde{\lambda}_i - \lambda_i\right) b_i.$$

As $v - \widetilde{v} \in \Lambda$, we have $|\widetilde{\lambda}_i - \lambda_i| \in \mathbb{Z}$ for $i \in [\ell]$. But $|\widetilde{\lambda}_i - \lambda_i| < 1$ for $i \in [\ell]$ implies $\widetilde{\lambda}_i - \lambda_i = 0$ for $i \in [\ell]$. This implies $y = \widetilde{y}$ and we conclude $v = \widetilde{v}$. □

Corollary 2.6.
Let $\Lambda \subset \mathbb{R}^d$ be a lattice with lattice basis $\mathcal{B}$ and fundamental parallelepiped $\Pi_\mathcal{B}$. Then $\mathsf{span}_\mathbb{R}(\Lambda)$ is the disjoint union of Λ-translates $\Pi_\mathcal{B} + u = \{x + u \mid x \in \Pi_\mathcal{B}\}$, that is, $\mathsf{span}_\mathbb{R}(\Lambda) = \bigsqcup_{u\in\Lambda} (\Pi_\mathcal{B} + u)$.

2.2. **Sub-lattices and determinants.**
We first show an important metric invariant of a lattice $\Lambda \subset \mathbb{R}^d$: the volume of a fundamental parallelepiped of Λ does not depend on the choice of the lattice basis.

Theorem 2.7.
Let $\Lambda \subset \mathbb{R}^d$ be a lattice and $\mathcal{B} = \{b_1, \dots, b_\ell\}$ and $\widetilde{\mathcal{B}} = \{\widetilde{b}_1, \dots, \widetilde{b}_\ell\}$ two lattice bases for Λ. Then $\mathsf{vol}_{\mathbb{R}^d}(\Pi_\mathcal{B}) = \mathsf{vol}_{\mathbb{R}^d}(\Pi_{\widetilde{\mathcal{B}}})$.

Proof. Clearly, the linear map $F : \mathsf{span}_{\mathbb{R}}(\mathcal{B}) \to \mathsf{span}_{\mathbb{R}}(\widetilde{\mathcal{B}})$ defined via $b_i \mapsto \widetilde{b}_i$ restricts to a lattice isomorphism $f : \Lambda \to \Lambda$ and it remains to show that $|\det(F)| = 1$.

We represent F by a matrix M with respect to the basis $\mathcal{B}$ and, since F is a lattice isomorphism, we know that $M \in \mathrm{Mat}(\ell \times \ell, \mathbb{Z})$. Similarly, F^{-1} is represented with respect to the basis $\mathcal{B}$ by $M^{-1} \in \mathrm{Mat}(\ell \times \ell, \mathbb{Z})$. Since the determinant is a polynomial in the entries of a matrix, we conclude that $\det(M), \det(M^{-1}) \in \mathbb{Z}$. Now $F \circ F^{-1} = \mathsf{Id}$ implies $|\det(F)| = |\det(M)| = 1$. □

Remark 2.8.

i) Notice that the proof of Theorem 2.7 relies on the fact that we consider a fixed lattice Λ.

ii) A matrix $M \in \mathrm{Mat}(\ell \times \ell, \mathbb{Z})$ with $|\det(M)| = 1$ is known as a unimodular matrix. The inverse M^{-1} clearly exists and satisfies $|\det(M^{-1})| = 1$. Moreover, Cramer's rule implies $M^{-1} \in \mathrm{Mat}(\ell \times \ell, \mathbb{Z})$. This is the reason why two lattices $\Lambda_1 \subset \mathbb{R}^{d_1}$ and $\Lambda_2 \subset \mathbb{R}^{d_2}$ are called unimodular equivalent if $\mathsf{rk}(\Lambda_1) = \mathsf{rk}(\Lambda_1)$ and their fundamental parallelepipeds have the same volume.

iii) There are infinitely many unimodular matrices in dimensions ≥ 2. As a consequence, there are infinitely many different bases for a given lattice $\Lambda \subset \mathbb{R}^d$ and it is useful to distinguish certain bases. For example, we shall consider the problem how to construct a basis that consists of short vectors (and be more precise what 'consists of short vectors' actually means).

Definition 2.9 (sub-lattice, index of sub-lattice)**.**
Let $\Lambda \subset \mathbb{R}^d$ be a lattice.

a) A sub-lattice of Λ is a lattice $\Gamma \subset \mathbb{R}^d$ that satisfies $\Gamma \subseteq \Lambda$.

b) Let Γ be a sub-lattice of Λ. A coset of Γ is a set $a + \Gamma = \{a + u \ \mid u \in \Gamma\}$ for some $a \in \Lambda$ and the set of all cosets of Γ is denoted by Λ/Γ. The index of Γ in Λ is the cardinality $|\Lambda/\Gamma|$ of Λ/Γ.

Given a sub-lattice Γ of a lattice $\Lambda \subset \mathbb{R}^d$, the set Λ/Γ is naturally endowed with an abelian group structure since Γ is a normal subgroup of Λ. Notice that Λ/Γ fails to be a lattice in general. Nevertheless it is rewarding to consider these more general quotient structures.

We now want to relate the volume of a fundamental parallelepiped of a sub-lattice Γ of Λ to the index $|\Lambda/\Gamma|$. More precisely, we show that lattice bases for Γ and Λ can be related in a particularly nice way. To that direction, we first prove a statement that resembles a statement on quotient spaces and their bases from linear algebra in the context of lattices.

Proposition 2.10.
Let $\Lambda \subset \mathbb{R}^d$ be a lattice with $V := \mathsf{span}_{\mathbb{R}}(\Lambda)$ and consider a nontrivial subspace $U \subseteq V$ that is generated by elements of Λ together with the quotient map $\pi_U : V \to V/U$.

i) $\pi_U(\Lambda) \subset V/U$ is a lattice.

ii) Let $\{b_1, \dots b_r\}$ be a lattice basis of the lattice $\Lambda \cap U$ and $\{c_1, \dots c_s\}$ be a lattice basis of $\pi_U(\Lambda)$. Then there exist $\widetilde{c}_1, \dots \widetilde{c}_s \in \Lambda$ with $\pi_U(\widetilde{c}_i) = c_i$ for $i \in [s]$ such that

$$\mathcal{B} := \{b_1, \dots b_r, \widetilde{c}_1, \dots \widetilde{c}_s\}$$

is a lattice basis of Λ. In particular, we have $\ell = r + s$.

We also use the short hand Λ/U for the quotient lattice $\pi_U(\Lambda)$ if the assumptions of the proposition are fulfilled. Notice that $\mathsf{rk}(\Lambda) = \dim(U)$ implies that Λ/U is the trivial lattice $\{0 + U\} \subset V/U = V/V$ with $\varnothing$ as lattice basis even.

Proof. To show that $\pi_U(\Lambda)$ is a lattice, we first remark that $\pi_U(\Lambda)$ is a subgroup of the vector space V/U as π_U is known to be a homomorphism of vector spaces from linear algebra. It is a bit harder to argue that $\pi_U(\Lambda)$ is discrete in V/U. Recall that we have to show that for all $x \in \Lambda/U$ there is a $\varepsilon > 0$ such that $B_\varepsilon(x) \cap \Lambda/U = \{x\}$. It suffices to check this property for $x = 0 + U$.

Since U is generated by elements of Λ, there is a basis $\{b_1, \dots b_r\} \subset \Lambda \cap U$ of U that extends to a basis $\{b_1, \dots b_\ell\} \subset \Lambda$ of V. We consider the maximum norm with respect to these bases on V as well as V/U, that is, we define

$$\left\| \sum_{i \in [\ell]} \lambda_i b_i \right\|_V := \max \left\{ |\lambda_i| \ \mid i \in [\ell] \right\}$$

and

$$\left\| \sum_{i\in[\ell]\setminus[r]} \lambda_i b_i + U \right\|_{V/U} := \max\left\{ |\lambda_i| \;\middle|\; i \in [\ell]\setminus[r] \right\}.$$

If B_V denotes the unit ball in V centred at 0 with respect to $\| \ \|_V$ then B_V is compact which in turn implies that $B_V \cap \Lambda$ is finite. Moreover, notice that

$$\varepsilon := \min\left(\{1\} \cup \left\{ \|x+U\|_{V/U} \;\middle|\; x \in B_V \cap V \setminus U \right\}\right)$$

is positive since ε is a minimum of positive integers.

We now claim that $x \in \Lambda$ with $\|x+U\|_{V/U} < \varepsilon$ implies $x+U = 0+U$ in V/U. Therefore consider $x = \sum_{i\in[\ell]} \lambda_i b_i \in \Lambda$ with $\|x+U\|_{V/U} < \varepsilon$ and define $\widetilde{x} := x - \sum_{i=1}^{r} \lfloor \lambda_i \rfloor b_i$. Clearly, we have $x+U = \widetilde{x}+U$ in V/U and, as $\varepsilon \leq 1$, we conclude $\widetilde{x} \in B_V \cap \Lambda$. The definition of ε now implies $\widetilde{x} \in U$, that is, $\widetilde{x}+U = 0+U$ in V/U.

To prove *ii*), let $\{b_1, \dots b_r\}$ and $\{c_1, \dots c_s\}$ as stated. If $s = 0$ there is nothing to show, so we assume $s > 1$ and choose $\widetilde{c}_1, \dots \widetilde{c}_s \in \Lambda$ with $\pi_U(\widetilde{c}_i) = c_i$ for $i \in [s]$ (they clearly exist) and let $x \in \Lambda$. As $\{c_1, \dots c_s\}$ is a lattice basis of $\pi_U(V)$, there are integers λ_i such that $\pi_U(x) = \sum_{i\in[s]} \lambda_i c_i$. Hence $x - \sum_{i\in[s]} \lambda_i \widetilde{c}_i \in \ker(\pi_U) = U$. As $\{b_1, \dots, b_r\}$ is a lattice basis of $\Lambda \cap U$, we have $x - \sum_{i\in[s]} \lambda_i \widetilde{c}_i = \sum_{i\in[r]} \mu_i b_i$ where $\mu_i \in \mathbb{Z}$ for $i \in [r]$. We conclude that Λ is generated by $\{b_1, \dots b_r, \widetilde{c}_1, \dots \widetilde{c}_s\}$. This set is linearly independent by a dimension argument. □

Definition 2.11 (primitive vector)**.**
Let $\Lambda \subset \mathbb{R}^d$ be a lattice. A Λ-primitive vector is a nontrivial lattice vector $x \in \Lambda$ that is not the positive integer multiple of any other lattice vector, this is, $(\lambda = 1, v = x)$ and $(\lambda = -1, x = -x)$ are the only solutions of the equation $x = \lambda v$ with unknowns $\lambda \in \mathbb{Z}$ and $v \in \Lambda$.

To illustrate this notion, consider the lattice $\mathbb{Z}^d \subset \mathbb{R}^d$ and notice that vector $v \in \mathbb{Z}^d$ is primitive if and only if $\gcd(v_1, \dots, v_d) = 1$. It turns out that the notion of a primitive vector is quite useful. For example, $\{v\}$ is a basis of a lattice $\Lambda \subset \mathbb{R}^d$ of rank 1 if and only if v is primitive. Clearly, if $\mathsf{rk}(\Lambda) > 1$ then any lattice basis is a set of primitive vectors but the converse is not true.

Theorem 2.12.
Let Γ be a sub-lattice of the lattice $\Lambda \subset \mathbb{R}^d$ with $\mathsf{rk}(\Gamma) = \mathsf{rk}(\Lambda)$. Then there exist a lattice basis $\mathcal{B}_\Lambda = \{b_1, \dots, b_\ell\}$ and positive integers $\alpha_1, \dots, \alpha_\ell$ with $\alpha_i | \alpha_{i-1}$ for $i \in [\ell] \setminus \{1\}$ such that

$$\mathcal{B}_\Gamma := \{\alpha_1 b_1, \dots, \alpha_\ell b_\ell\}$$

is a lattice basis for Γ.

Proof. We prove this theorem by induction on $\ell = \mathsf{rk}(\Lambda) = \mathsf{rk}(\Gamma)$. If $\ell = 1$, let $\{b_1\}$ and $\{c_1\}$ be a lattice basis of Λ and Γ. As $\Gamma \subset \Lambda$, there exists an integer α_1 such that $c_1 = \alpha_1 b_1$. Then $\{|\alpha_1| \cdot b_1\}$ is a lattice basis of Γ.

Assume now that $\ell \geq 2$. As $\mathsf{rk}(\Lambda) = \mathsf{rk}(\Gamma)$ and $\Gamma \subset \Lambda$, there exist for every $x \in \Lambda$ a smallest positive integer α_x such that $\alpha_x x \in \Gamma$. After a possible relabelling of $\mathcal{B}_\Lambda$, we assume that α_ℓ for b_ℓ is minimal for all elements of $\mathcal{B}_\Lambda$. Moreover, among all bases $\mathcal{B}_\Lambda$ of Λ, we choose $\mathcal{B}_\Lambda$ such that the corresponding α_ℓ is minimal. If we now set $U := \mathsf{span}_{\mathbb{R}}(b_\ell)$ then b_ℓ is a lattice basis of $\Lambda \cap U$ and $\alpha_\ell b_\ell$ is a lattice basis for $\Gamma \cap U$. By Proposition 2.10, we know that $\Gamma/U \subseteq \Lambda/U$ are lattices of rank $\ell - 1$ and, by induction hypothesis, we have a lattice basis $\{\widetilde{b}_1, \dots, \widetilde{b}_{\ell-1}\}$ of Λ/U together with positive integers $\alpha_1, \dots, \alpha_{\ell-1}$ such that $\alpha_i | \alpha_{i+1}$ for $i \in [\ell - 1]$ and $\{\alpha_1 \widetilde{b}_1, \dots, \alpha_{\ell-1}\widetilde{b}_{\ell-1}\}$ is a lattice basis of Γ/U.

Now choose representatives $b_i \in \Lambda$ for each $\widetilde{b}_i$ and representatives $\widetilde{c}_i \in \Gamma$ for each $\alpha_i \widetilde{b}_i$. Then Proposition 2.10 implies that $\{b_1, \dots, b_\ell\}$ and $\{\widetilde{c}_1, \dots, \widetilde{c}_{\ell-1}, \alpha_\ell b_\ell\}$ form lattice bases of Λ and Γ. Moreover, for every $i \in [\ell - 1]$ there exist $\beta_i \in \mathbb{Z}$ such that $c_i := \widetilde{c}_i + \beta_i(\alpha_\ell b_\ell) = \alpha_i b_i + \gamma_i b_\ell$ with $0 \leq \gamma_i < \alpha_r$. We now claim that $\gamma_i = 0$ for $i \in [\ell - 1]$.

As Γ is a sub-lattice of Λ with $\mathsf{rk}(\Gamma) = \mathsf{rk}(\Lambda)$, we know that for each c_i there exists a positive integer δ_i and a primitive vector $v_i \in \Lambda$ such that $c_i = \delta_i v_i$. Now $\delta_i v_i = \alpha_i b_i + \gamma_i b_\ell$ implies either $\gamma_i = 0$ or $\delta_i \leq \gamma_i < \alpha_i$. But $\delta_i \leq \gamma_i < \alpha_i$ is impossible by our choice of $\mathcal{B}_\Lambda$. □

Corollary 2.13.
Let Γ be a sub-lattice of $\Lambda \subset \mathbb{R}^d$ such that $\mathsf{rk}(\Gamma) = \mathsf{rk}(\Lambda) = \ell$ and consider lattice bases $\mathcal{B}_\Lambda$ and $\mathcal{B}_\Gamma$ of Λ and Γ as described in Theorem 2.12. Then

$$|\Lambda/\Gamma| = |\Pi_{\mathcal{B}_\Gamma} \cap \Lambda| = \prod_{i\in[\ell]} \alpha_i.$$

Proof. The quotient map $\pi_\Gamma : \Lambda \to \Lambda/\Gamma$ is defined via $x \mapsto x + \Gamma$ and induces a bijection $\varphi : \Pi_{\mathcal{B}_\Gamma} \cap \Lambda \to \Lambda/\Gamma$ by Proposition 2.5: since $\mathsf{rk}(\Gamma) = \mathsf{rk}(\Lambda)$, we find a unique representative $x \in \Pi_{\mathcal{B}_\Gamma} \cap \Lambda$ for every coset $x + U$. This proves the first equality.

This geometric point of view also proves the second equality: $\Pi_{\mathcal{B}_\Gamma}$ is simply a dilation of $\Pi_{\mathcal{B}_\Lambda}$ by Theorem 2.12 and $|\Pi_{\mathcal{B}_\Gamma} \cap \Lambda|$ is the number of copies of $\Pi_{\mathcal{B}_\Lambda}$ that are needed to tile $\Pi_{\mathcal{B}_\Gamma}$. The corresponding volume deformation is described by the linear map $F : \mathsf{span}_{\mathbb{R}}(\Lambda) \to \mathsf{span}_{\mathbb{R}}(\Lambda)$ defined via $b_i \mapsto \alpha_i b_i$ for $i \in [\ell]$ which restricts to a lattice isomorphism $f : \Lambda \to \Gamma$. □

Corollary 2.14.
Let Γ be a sub-lattice of a lattice $\Lambda \subset \mathbb{R}^d$. Then $|\Lambda/\Gamma|$ is finite if and only if $\mathsf{rk}(\Lambda) = \mathsf{rk}(\Gamma)$.

Corollary 2.15.
Let $\mathcal{B} = \{v_1, \dots, v_d\} \subset \mathbb{Z}^d$ be linearly independent vectors and $\Lambda \subset \mathbb{R}^d$ the lattice generated by the vectors of $\mathcal{B}$. Then the number of integer points contained in $\Pi_\mathcal{B}$ equals the volume of $\Pi_\mathcal{B}$:

$$|\Pi_\mathcal{B} \cap \mathbb{Z}^d| = |\det(M_\mathcal{B})|$$

where $M_\mathcal{B}$ is the matrix with columns $v_1, \dots, v_d$.

Proof. The claim is a direct consequence of Corollary 2.13 since Λ is a sub-lattice of the lattice $\mathbb{Z}^d \subset \mathbb{R}^d$ and the volume $\mathsf{vol}_{\mathbb{R}^d}(\Pi_{\mathbb{Z}^d}) = 1$. □

3. Basics on cones

Besides polytopes and lattices, cones are the third class of fundamental objects we shall use to describe functions (in fact polynomials) that count the number of lattice points of dilates of a lattice polytope. Similar to polytopes and lattices, we give two possible definitions: we define finitely constrained and finitely generated cones. The Weyl-Minkowski Theorem then tells us that these definitions do coincide.

Definition 3.1.
a) A subset $C \subset \mathbb{R}^d$ is a cone if and only if $x, y \in C$ and $\lambda, \mu \in \mathbb{R}_{\geq}$ implies $\lambda x + \mu y \in C$.
b) A cone C is polyhedral (or finitely constrained) if and only if there exist linear functionals $\alpha_1, \ldots, \alpha_m \in (\mathbb{R}^d)^*$ such that

$$C = \left\{ x \in \mathbb{R}^d \;\middle|\; \alpha_i(x) \leq 0 \text{ for all } i \in [m] \right\}.$$

c) A cone C is finitely generated by $\mathcal{B}_C = \{v_1, \ldots, v_r\} \subset \mathbb{R}^d$ if and only if

$$C = \mathsf{cone}(\mathcal{B}_C) := \left\{ \textstyle\sum_{i \in [d]} \lambda_i v_i \;\middle|\; \lambda_i \in \mathbb{R}_{\geq} \text{ for } i \in [d] \right\}.$$

It is easy to check that every polyhedral and every finitely generated cone is in fact a cone. Moreover, we have $0 \in C$ for every cone C.

Theorem 3.2 (Minkowski-Weyl duality for cones)**.**
A cone C is polyhedral if and only if C is finitely generated.

We split Theorem 3.2 into its its two implications. We first prove '$\Leftarrow$' (Weyl's Theorem, theorem 3.4) and then prove '$\Rightarrow$' (Minkowski's Theorem, theorem 3.11). For Weyl's Theorem, we warm up using the Fourier-Motzkin elimination to prove the following lemma.

Lemma 3.3. *Let $C \subset \mathbb{R}^{d+1}$ be a polyhedral cone and $\pi : \mathbb{R}^{d+1} \to \mathbb{R}^d$ be a projection that forgets one coordinate. Then $\pi(C)$ is a polyhedral cone.*

Proof. Let $C \subset \mathbb{R}^{d+1}$ be a polyhedral cone defined by

$$C := \left\{ (x_0, x) \in \mathbb{R}^{d+1} \;\middle|\; \lambda_i x_0 + \alpha_i(x) \leq 0 \text{ for } i \in m \right\}$$

where $\alpha_i \in (\mathbb{R}^d)^*$ and $\lambda_i \in \mathbb{R}$ for $i \in [m]$. Without loss of generality, we suppose that π forgets about the x_0-direction and set

$$C' := \pi(C) = \left\{ x \in \mathbb{R}^d \;\middle|\; (x_0, x) \in C \text{ for some } x_0 \in \mathbb{R} \right\}.$$

After possible relabelling, we may assume that there exist $a, b \in \mathbb{N}_0$ such that

$$\lambda_i \in \begin{cases} \{0\} & \text{if } 0 < i \leq a, \\ \mathbb{R}_+ & \text{if } a < i \leq b, \\ \mathbb{R}_- & \text{if } b < i \leq m. \end{cases}$$

Moreover, for $a < i \leq b < j \leq m$, we define linear functionals $\beta_{ij} \in (\mathbb{R}^d)*$ as

$$\beta_{ij}(x) := \lambda_i \alpha_j(x) - \lambda_j \alpha_i(x)$$

and

$$D := \left\{ x \in \mathbb{R}^d \;\middle|\; \begin{array}{c} \alpha_i(x) \leq 0 \text{ for } 0 < i \leq a \\ \beta_{ij}(x) \leq 0 \text{ for } a < i \leq b < j \leq m \end{array} \right\}.$$

We claim that $C' = D$. As '$C' \subseteq D$' is obvious (the defining inequalities of D are linear combinations of defining inequalities of C'), it reamins to show $D \subseteq C'$. So let $x \in D$ and distinguish two cases.
i) $0 < i \leq a$.
Then $\lambda_i x_0 + \alpha_i(x) \leq 0$ for all $x_0 \in \mathbb{R}$ as $\lambda_i = 0$.

ii) $a < i \leq b < j \leq m$.
Then $\beta_{ij}(x) \leq 0$ can be rewritten as $\frac{1}{\lambda_j}\alpha_j(x) \geq \frac{1}{\lambda_i}\alpha_i(x)$ and there exists $x_0 \in \mathbb{R}$ such that

$$\min_{b<j\leq m}\left(\tfrac{1}{\lambda_j}\alpha_j(x)\right) \leq -x_0 \leq \max_{0<i\leq b}\left(\tfrac{1}{\lambda_i}\alpha_i(x)\right).$$

This clearly implies

$$\lambda_i x_0 + \alpha_i(x) \leq 0 \text{ for } a < i \leq b \qquad \text{and} \qquad \lambda_j x_0 + \alpha_j(x) \leq 0 \text{ for } b < j \leq m.$$

But this shows that $(x_0, x) \in C$ which in turn proves that $x \in C'$.

□

Theorem 3.4 (Weyl's Theorem)**.**
If a cone C is finitely generated then it is polyhedral.

Proof. Consider $C = \left\{\sum_{i\in[r]} \lambda_i v_i \in \mathbb{R}^d \;\middle|\; \lambda_1, \ldots, \lambda_r \in \mathbb{R}_{\geq}\right\}$, that is, C is generated by finitely many vectors $v_1, \ldots, v_r \in \mathbb{R}^d$. Now consider

$$C' := \left\{(\lambda_1, \ldots, \lambda_r, x) \in \mathbb{R}^{r+d} \;\middle|\; \begin{smallmatrix}\lambda_i \geq 0 \text{ for } i\in[r] \\ x - \sum_{i\in[r]} \lambda_i v_i = 0\end{smallmatrix}\right\}$$

which is a finitely constrained cone. Since C' projects to C (by forgetting the first r coordinates), we repeatedly apply Lemma 3.3 to conclude that C is also polyhedral. □

Theorem 3.5 (Farkas' Lemma)**.**
Let C be a cone that is finitely generated by $v_1, \ldots, v_r \in \mathbb{R}^d$ and $x \in \mathbb{R}^d$. Then precisely one of the following statements is true:
i) $x \in C$.
ii) There exists $\alpha \in (\mathbb{R}^d)^*$ such that $x \notin H_\alpha^-$ and $C \subseteq H_\alpha^-$ where $H_\alpha^- := \left\{z \in \mathbb{R}^d \;\middle|\; \alpha(z) \leq 0\right\}$.

The geometric meaning of the second statement of the Farkas' Lemma can is rephrased as follows. For every $x \in \mathbb{R}^d \setminus C$ there exists a linear hyperplane $H_\alpha := \left\{z \in \mathbb{R}^d \;\middle|\; \alpha(z) = 0\right\}$ that separates x from the cone C. We say that the linear hyperplane H_α is a valid hyperplane of C if H_α separates some $x \in \mathbb{R}^d$ from C.

Proof. We first show that it is impossible that both statements are true at the same time. So we assume that $x \in C$, that is there exist $\lambda_1, \ldots, \lambda_r \geq 0$ with $x = \sum_{i\in[r]} \lambda_i v_i$, and that there exists $\alpha \in (\mathbb{R}^d)^*$ such that $\alpha(x) > 0$ and $\alpha(y) \leq 0$ for all $y \in C$. This yields the contradiction

$$0 < \alpha(x) = \alpha\left(\sum_{i\in[r]} \lambda_i v_i\right) = \sum_{i\in[r]} \lambda_i \alpha(v_i) \leq 0.$$

By Weyl's Theorem, the cone C is polyhedral, that is, there exist finitely many linear functionals $\alpha_1, \ldots, \alpha_m \in (\mathbb{R}^d)^*$ such that

$$C = \left\{y \in \mathbb{R}^d \;\middle|\; \alpha_i(y) \geq 0 \text{ for } i \in [m]\right\}.$$

Now $x \notin C$ holds if and only if there exists $j \in [m]$ with $\alpha_j(x) > 0$. Since for every $y \in C$ there exist $\lambda_1, \ldots, \lambda_r \geq 0$ such that $y = \sum_{i\in[r]} \lambda_i v_i$ and since $\alpha_j(v_i) \leq 0$ for all $i \in [r]$, we conclude

$$\alpha_j(y) = \alpha\left(\sum_{i\in[r]} \lambda_i v_i\right) = \sum_{i\in[r]} \lambda_i \alpha_j(v_i) \leq 0.$$

This shows that we can choose $\alpha = \alpha_j$ in the second statement. □

Definition 3.6 (polar dual cone)**.**
The polar dual of a cone $C \subset \mathbb{R}^d$ is the set

$$C^* := \left\{\alpha \in (\mathbb{R}^d)^* \;\middle|\; \alpha(x) \leq 0 \text{ for all } x \in C\right\}.$$

If $C = \mathsf{cone}\{v_1, \ldots, v_r\}$ is a finitely generated cone then it is immediate from the definition that it suffices to check $\alpha(x) \leq 0$ for $x \in \{v_1, \ldots, v_r\}$ to verify $\alpha \in C^*$. Using this, we obtain the following rephrasing of the Farkas' Lemma.

Corollary 3.7 (Farkas' Lemma (polar version))**.**
Let $C \subset \mathbb{R}^d$ be a finitely generated cone and $x \in \mathbb{R}^d$. Then precisely one of the following statements is true:
i) $x \in C$.
ii) There exists $\alpha \in C^*$ such that $\alpha(y) \leq 0$ for all $y \in C$ and $\alpha(x) > 0$.

Proposition 3.8. *If $C = \mathsf{cone}(v_1, \ldots, v_r) \subset R^d$ is a finitely generated cone then*

$$C^* := \left\{\alpha \in (\mathbb{R}^d)^* \;\middle|\; \alpha(v_i) \leq 0 \text{ for all } i \in [r]\right\}.$$

In particular, C^* is a polyhedral cone if C is finitely generated.

Proof. If $\alpha \in C^*$ then $\alpha(x) \leq 0$ for all $x \in C$ by defintion. In particular, $\alpha(v_i) \leq 0$ for all $i \in [r]$. This shows '$\subseteq$'.

Conversely, consider $\alpha \in (\mathbb{R}^d)^*$ such that $\alpha(v_i) \leq 0$ for all $i \in [r]$. If $\lambda_i \geq 0$ for all $i \in [r]$ then

$$\alpha\left(\textstyle\sum_{i\in[r]} \lambda_i v_i\right) = \sum_{i\in[r]} \lambda_i \alpha(v_i) \geq 0.$$

This proves $\alpha \in C^*$. □

Recall from linear algebra that $(\mathbb{R}^{d*})^*$ is isomorphic to $\mathbb{R}^d$, the standard identification satisfies $(v^*)^*(\alpha) = \alpha(v)$ for all $v \in \mathbb{R}^d$ and all $\alpha \in \mathbb{R}^{d*}$. One might expect that $(C^*)^* = C$ for all cones under this identification of $(\mathbb{R}^{d*})^*$ and $\mathbb{R}^d$, but this is not true in general.

Lemma 3.9. *If $C \subset \mathbb{R}^d$ is a finitely generated cone then $(C^*)^* = C$.*

Proof. Consider a finitely generated cone $C = \mathsf{cone}\{v_1, \ldots, v_r\}$. Then

$$C^* = \left\{\alpha \in \mathbb{R}^{d*} \;\middle|\; (v_i^*)^*(\alpha) \leq 0 \text{ for all } i \in [r]\right\}.$$

As $x \in C$ implies $\alpha(x) \leq 0$ for all $\alpha \in C^*$, we have $(x^*)^*(\alpha) \leq 0$ for all $\alpha \in C^*$. This shows that $x \in (C^*)^*$.

Conversely, if $x \notin C$ then the dual version of the Farkas' Lemma (Corollary 3.7) implies that there exists $\alpha \in C^*$ such that $\alpha(v_i) \leq 0$ for all $i \in [r]$ and $\alpha(x) > 0$. This shows $x \notin (C^*)^*$. □

In particular, we obtain the following description of the polar dual of a finitely generated cone.

Corollary 3.10. *If $C = \left\{x \in \mathbb{R}^d \;\middle|\; \alpha_i(x) \leq 0 \text{ for } i \in [m]\right\}$ is a finitely constrained cone then the polar dual cone C^* of C is finitely generated:*

$$C^* = \mathsf{cone}\{\alpha_1, \ldots, \alpha_m\}.$$

We are now able to prove the missing implication of the Weyl-Minkowsky Theorem for cones.

Theorem 3.11 (Minkowski's Theorem for cones)**.**
If $C \subset \mathbb{R}^d$ is a polyhedral cone then C is a nonempty finitely generated cone.

Proof. Consider a finitely constrained cone $C = \left\{x \in \mathbb{R}^d \;\middle|\; \alpha_i(x) \leq 0 \text{ for } i \in [m]\right\}$. Then $0 \in C$ which proves $C \neq \varnothing$.

Additionally to C, consider the finitely generated cone $D := \mathsf{cone}\{\alpha_1, \ldots, \alpha_m\} \subset \mathbb{R}^{d*}$. Then $D = C^*$ by Corollary 3.10 and we conclude that D is a polyhedral cone by Weyl's Theorem (Theorem 3.4). Thus there exist $(v_1^*)^*, \ldots, (v_r^*)^* \in (\mathbb{R}^{d*})^* = \mathbb{R}^d$ such that

$$D = \left\{\alpha \in (\mathbb{R}^d)^* \;\middle|\; (v_i^*)^*(\alpha) = \alpha(v_i) \leq 0 \text{ for } i \in [r]\right\}.$$

Now the is the polar dual of $D \subset \mathbb{R}^{d*}$ is the finitely generated cone $(E^*)^* := \mathsf{cone}\{(v_1^*)^*, \ldots, (v_r^*)^*\}$ which implies $E^* = D$. This shows $C = E$ and we conclude that C is finitely generated. □

Definition 3.12 (Minkowski sum)**.**
The Minkowski sum $A + B$ of two sets $A, B \subset \mathbb{R}^d$ is defined as

$$A + B := \{a + b \mid a \in A \text{ and } b \in B\}.$$

Definition 3.13 (lineality space)**.**
The lineality space lineal(C) of a polyhedral cone $C \subset R^d$ is defined as

$$\text{lineal}(C) := \left\{ y \in \mathbb{R}^d \;\middle|\; x + \lambda y \in C \text{ for all } x \in C \text{ and all } \lambda \in \mathbb{R} \right\}.$$

The cone C is called pointed if $\text{lineal}(C) = \{0\}$.

Consider now a polyhedral cone $C \subset \mathbb{R}^d$, its lineality space $\text{lineal}(C)$ and a complimentary subspace W of L in $\mathbb{R}^d$. Moreover, denote the projection of C onto W by D. Then D is a cone such that $C = L + D$ and $\text{lineal}(D) = \{0\}$. Hence, up to Minkowski sum with a linear space, we may consider pointed cones only. A pointed cone C can also be characterized by the property that there exists $\alpha \in \mathbb{R}^{d*}$ such that $\alpha(x) < 0$ for all $x \in C \setminus \{0\}$.

Lemma 3.14. *Let $C \subset \mathbb{R}^d$ be a polyhedral cone. Then C is pointed if and only if there exists a linear functional $\alpha \in \mathbb{R}^{d*}$ such that $\alpha(x) < 0$ for all $x \in C \setminus \{0\}$.*

Proposition 3.15.
If $C = \left\{ x \in \mathbb{R}^d \;\middle|\; \alpha_i(x) \leq 0 \text{ for all } i \in [m] \right\}$ then

$$\text{lineal}(C) = \left\{ y \in \mathbb{R}^d \;\middle|\; \alpha_i(y) = 0 \text{ for all } i \in [m] \right\}.$$

Proof. We have $\left\{ y \in \mathbb{R}^d \;\middle|\; \alpha_i(y) = 0 \text{ for all } i \in [m] \right\} \subseteq \text{lineal}(C)$ by definition.

Conversely, let $y \in \text{lineal}(C)$ and $x \in C$. If there exists $j \in [m]$ such that $\alpha_j(y) \neq 0$ then $0 \geq \alpha_j(x + \lambda y) = \alpha_j(x) + \lambda(y) > 0$ for sufficiently large $\lambda \in \mathbb{R}$. As this is impossible, we conclude that $\alpha_i(y) = 0$ for all $y \in \text{lineal}(C)$. This proves $\text{lineal}(C) \subseteq \left\{ y \in \mathbb{R}^d \;\middle|\; \alpha_i(y) = 0 \text{ for all } i \in [m] \right\}$ □

We now prove the first result that relates polyhedral cones and lattices: the existence of a Hilbert basis. If $C \subset \mathbb{R}^d$ is a polyhedral cone and $\Lambda \subset \mathbb{R}^d$ is a lattice such that $C \subset \mathsf{span}_{\mathbb{R}}\Lambda$ then consider $S_C := C \cap \Lambda$, the set of all lattice points in C. Notice that S_C is a semi-group because S_C is closed under addition and $0 \in S_C$.

Definition 3.16. A Hilbert basis $\mathcal{H}$ is a subset of the semi-group S_C such that $x \in \mathsf{span}_{\mathbb{N}_0}\mathcal{H}$ for every $x \in S_C$, that is, if $x = \sum_{h \in \mathcal{H}} \mu_h h$ with $\mu_h \in \mathbb{N}_0$ for every $x \in S_C$. A Hilbert basis $\mathcal{H}$ is a minimal Hilbert basis if no proper subset of $\mathcal{H}$ is a Hilbert basis.

Notice that a Hilbert basis of S_C is not a basis of Λ in general and that the cardinality of a minimal Hilbert basis is not determined by C and Λ. For example, consider $C = \mathbb{R}^2$ and $\Lambda = \mathbb{Z}^2$. Then $\{e_1, e_2, -(e_1 + e_2)\}$ as well as $\{\pm e_1, \pm e_2\}$ is a minimal Hilbert basis of $S_C = \mathbb{R}^2 \cap \mathbb{Z}^2$.

We now prove the existence of a Hilbert basis $\mathcal{H}$ of S_C and construct a minimal Hilbert basis if C is a pointed cone. To simplify the argument, we restrict to the standard lattice $\Lambda = \mathbb{Z}^d \subset \mathbb{R}^d$.

Theorem 3.17. *(Existence of Hilbert bases)*
Let $\Lambda = \mathbb{Z}^d \subset \mathbb{R}^d$ be a lattice, $C \subseteq \mathbb{R}^d$ a polyhedral cone generated by $\{v_1, \ldots, v_r\} \subset \Lambda$ and $S_C := C \cap \Lambda$ the semi-group of lattice points contained in C. Then there exists a Hilbert basis of S_C. Moreover, if C is a pointed cone then there exists a unique minimal Hilbert basis.

Proof. Let Π denote the closed parallelepiped spanned by $v_1, \ldots, v_r$, that is,

$$\Pi := \left\{ \textstyle\sum_{i \in [r]} \lambda_i v_r \in \mathbb{R}^d \;\middle|\; 0 \leq \lambda_i \leq 1 \text{ for } i \in [r] \right\},$$

and set $\mathcal{H} := \Pi \cap \Lambda$. We claim that $\mathcal{H}$ is a Hilbert basis of S_C.

Since $v_1, \ldots, v_r \in \mathcal{H}$, we conclude that $\mathcal{H}$ generates C and it remains to show that any lattice vector $x \in S_C$ is a linear combination of vectors of $\mathcal{H}$ where all coefficients are nonnegative integers. If $x \in S_C$ then $x = \sum_{i \in [r]} \eta_i v_i$ for some $\eta_1, \ldots, \eta_r \in \mathbb{R}_{\geq}$. Thus

$$x - \textstyle\sum_{i \in [r]} \lfloor \eta_i \rfloor v_i = \sum_{i \in [r]} (\eta_i - \lfloor \eta_i \rfloor) v_i \in \Lambda.$$

Moreover, $0 \leq (\eta_i - \lfloor \eta_i \rfloor) < 1$ for all $i \in [r]$, so this lattice point is contained in $\Pi \cap \Lambda$. This implies that x is an integral conic combination of $\mathcal{H}$, that is, $\mathcal{H}$ is a Hilbert basis of S_C.

We now assume that C is a pointed polyhedral cone that is generated by $\{v_1, \ldots, v_r\} \subset \Lambda$ and construct a minimal Hilbert basis of C. First, Lemma 3.15 implies that there exists a linear functional $\alpha \in \mathbb{R}^{d*}$ such that $\alpha(x) > 0$ for all $x \in C \setminus \{0\}$. Next define

$$K := \left\{ y \in S_C \setminus \{0\} \;\middle|\; y \neq a + b \text{ for } a, b \in S_C \setminus \{0\} \right\}.$$

As $\mathcal{H}$ is bounded, we conclude that $K \subseteq \mathcal{H}$ is finite, that is, $K = \{\kappa_1, \ldots, \kappa_s\}$. Moreover, define

$$M := \left\{ x \in S_C \;\middle|\; x \neq \textstyle\sum_{i\in[s]} \mu_i \kappa_i \text{ for } \mu_i \in \mathbb{N}_0 \right\}.$$

If K is not a Hilbert basis then $M \neq \varnothing$ and there exists $m_0 \in M$ with $\alpha(m_0) = \inf_{m\in M} \alpha(m)$. Clearly, $m_0 \notin K$, so there exist $x_1, x_2 \in S_C \setminus \{0\}$ with $m_0 = x_1 + x_2$. Then

$$\alpha(x_1) > 0, \qquad \alpha(x_2) > 0, \qquad \alpha(m_0) > 0 \qquad \text{and} \qquad \alpha(m_0) = \alpha(x_1) + \alpha(x_2)$$

imply that $\alpha(m_0) > \alpha(x_1)$ and $\alpha(m_0) > \alpha(x_1)$ which contradicts the choice of m_0. Thus K must be a Hilbert basis of S_C. On the other hand, let $a \in K$. Then a is not an integral conic combination of $K \setminus \{a\}$, so K is a minimal Hilbert basis. □

We end this subsection on cones by introducing faces of a cone and fans.

Definition 3.18.
A nontrivial face F of a polyhedral cone C is the intersection of C with a valid linear hyperplane H_α. Moreover, we consider $\varnothing$ and C as trivial faces of C.

The definition of a face immediately implies that $F \cap P = \mathsf{span}_{\mathbb{R}}(F) \cap P$ for any face F of the polyhedral cone C and we define the dimension of F as $\dim(F) = \dim(\mathsf{span}_{\mathbb{R}}(F))$. Moreover, we have that any face of a polyhedral cone is again a polyhedral cone.

Definition 3.19. A finite family $\mathcal{F} = \{C_1, \ldots, C_N\}$ of nonempty cones in $\mathbb{R}^d$ is a fan in $\mathbb{R}^d$ if it satisfies

i) Every nonempty face of a cone in $\mathcal{F}$ is also a cone in $\mathcal{F}$.
ii) The intersection of any two cones in $\mathcal{F}$ is a face of both.

A fan $\mathcal{F}$ is a complete fan if $\bigcup_{C\in\mathcal{F}} C = \mathbb{R}^d$.

4. Basics on polytopes

5. Ehrhart theory: counting lattice points of cones

We aim for functions that count lattice points of dilates of a lattice polytope P. More precisely, such a function will be a polynomial in one variable (the dilation factor). But before we discuss the situation for polytopes, we count lattice points for polyhedral cones. To simplify the exposition, we consider the standard integer lattice $\Lambda = \mathbb{Z}^d \subset \mathbb{R}^d$ unless otherwise stated.

5.1. First examples and tools.

Definition 5.1. The Ehrhart counting function $\mathsf{ehr}_S : \mathbb{N} \to \mathbb{N}$ of a bounded set $S \subseteq \mathbb{R}^d$ is defined via $t \mapsto |tS \cap \mathbb{Z}^d|$.

Example 5.2.

a) The line segment $[a, b] \subset \mathbb{R}$.
Let $S := [a, b]$ with $a, b \in \mathbb{R}$ and $a \leq b$. Then S contains $\lfloor b \rfloor - \lceil a \rceil + 1$ lattice points while the t^{th}-dilate tS contains $\lfloor tb \rfloor - \lceil ta \rceil + 1$ lattice points. If $a, b \in \mathbb{Z}$ then the Ehrhart counting function simplifies to
$$\mathsf{ehr}_S(t) = (b - a)t + 1.$$
Notice that $\mathsf{ehr}_S(t)$ is a polynomial of degree 1 in one variable with leading coefficient $(b - a)$ which is the 1-dimensional volume of S.

b) The d-dimensional standard simplex Δ_d.
The standard simplex Δ_d is a particular realization of a d-simplex in $\mathbb{R}^d$:
$$\Delta_d = \mathsf{conv}\{0, e_1, e_2, \ldots, e_d\} = \left\{ x \in \mathbb{R}^d \;\middle|\; \begin{smallmatrix} x_i \geq 0 \text{ for all } i \in [d] \\ \sum_{i \in [d]} x_i \leq 1 \end{smallmatrix} \right\}.$$
We claim that
$$\mathsf{ehr}_{\Delta_d}(t) = \binom{d+t}{d} = \frac{(d+t)(d+t-1) \cdot \ldots \cdot (t+1)}{d!}$$
and notice that ehr_{Δ_d} is a polynomial of degree d in one variable t with leading coefficient $\frac{1}{d!}$ which is the d-dimensional volume of Δ_S.

The crucial ingredient to derive this formula of the Ehrhart counting function ehr_{Δ_d} is the following bijection between the lattice points $t\Delta_d \cap \mathbb{Z}^d$ and sequences of t dots and d bars: to each such sequence, assign a point $x \in \mathbb{R}^d$ where coordinate x_i is the *number of dots between bar* $(i-1)$ *and bar* i (after adding adding a auxiliary bar 0 in front of the sequence). This identification yields points of $\mathbb{Z}^d$ with nonnegative coordinates that satisfy $\sum_{i \in [d]} x_i \leq t$.

c) The d-dimensional cube C_d.
The cube C_d is a particular realization of a d-cube in $\mathbb{R}^d$:
$$C_d := [0, 1]^d = \mathsf{conv}\left\{ \textstyle\sum_{i \in [d]} \epsilon_i e_i \;\middle|\; \epsilon \in \{0, 1\}^d \right\} = \left\{ x \in \mathbb{R}^d \;\middle|\; 0 \leq x_i \leq 1 \text{ for all } i \in [d] \right\}.$$
Counting lattice points for t^{th}-dilates tC_d is fairly simple, we have
$$\mathsf{ehr}_{C_d}(t) = (t+1)^d.$$
Again, we observe that $\mathsf{ehr}_{C_d}(t)$ is a polynomial in one variable t of degree$d$ with leading coefficient 1 which is the d-dimensional volume of C_d.

Definition 5.3 (polyhedral complexes)**.**

a) A polyhedral complex $\mathcal{C}$ is a finite family of polyhedra (the 'cells' of the complex $\mathcal{C}$) such that the following two properties are satisfied for all $P, Q \in \mathcal{C}$:
   i) If F is a face of P then $F \in \mathcal{C}$.
   ii) $F := P \cap Q$ is a face of P and of Q.
   A polyhedral complex is a polytopal complex if all cells are bounded. Cells of a polyhedral complex are often called faces.

b) A cell $P \in \mathcal{C}$ is maximal in$\mathcal{C}$ if it is not properly contained in any cell $Q \in \mathcal{C}$.

c) The dimension of a polyhedral complex $\mathcal{C}$ is $\dim \mathcal{C} := \max_{P \in \mathcal{C}} \dim(P)$. The set of all cells of dimension d of $\mathcal{C}$ is denoted by $\mathcal{C}_d$. Cells of dimension 0 are called vertices and cells of dimension 1 are called edges.

d) The polyhedral complex $\mathcal{C}$ is pure if all maximal cells have the same dimension.
e) Let $\mathcal{C}$ be a pure polyhedral complex and F be a face of $\mathcal{C}$. Then F is a facet of$\mathcal{C}$ if $\dim F = \dim \mathcal{C}$. Moreover, F is a ridge of $\mathcal{C}$ if $\dim F = \dim \mathcal{C} - 1$.
f) A polyhedral complex $\mathcal{S}$ is a subcomplex of the polyhedral complex $\mathcal{C}$ if every cell of $\mathcal{S}$ is a cell of $\mathcal{C}$.

Example 5.4.
a) Any cone C can be seen as a pure polyhedral complex $\mathcal{C}$ where each face of C is a cell of $\mathcal{C}$. This yields a polyhedral complex with precisely one maximal cell.

   Moreover, if $\mathcal{C}$ is the polyhedral complex associated to $C = \mathsf{cone}(\mathcal{B})$ generated by the linearly independent set $\mathcal{B} = \{v_1, \dots, v_d\} \subset \mathbb{R}^d$ then the number of k-dimensional cells of $\mathcal{C}$ is $|\mathcal{C}_k| = \binom{d}{k}$.
b) To any polytope P, we can associate at least two pure polytopal complexes in a natural way. First, we see P as the pure polytopal complex $\mathcal{C}$ where each face of P is a cell of $\mathcal{C}$. This is a complex of dimension $\dim(P)$ with precisely one maximal cell. Topologically, $\mathcal{C}$ is a ball of dimension d. Second, we can see P as the pure polytopal complex $\partial P := \mathcal{C} \setminus \{P\}$. This is a complex of dimension $d-1$. Topologically, ∂P is homeomorphic to a sphere of dimension $d-1$.

   It is commonly agreed that facets and ridges of a polytope P refer to facets and ridgets of the complex ∂P. For example, the complex ∂C_3 associated to the 3-dimensional cube C_3 consists of 6 facets, 12 ridges = 12 edges, 8 vertices and one empty cell.
c) Any complete fan $\mathcal{F}$ in $\mathbb{R}^d$ is a pure polyhedral complex of dimension d.

Definition 5.5 (generic points, near and far cones and parallelepipeds)**.**
Let $\mathcal{B} = \{v_1, \dots, v_d\} \subset \mathbb{R}^d$ be linearly independent and set $C_{\mathcal{B}} := \mathsf{cone}(\mathcal{B})$.
a) A point $x = \sum_{i\in[d]} \lambda_i v_i$ is generic with respect to $C_{\mathcal{B}}$ if $\lambda_i \neq 0$ for $i \in [d]$. We then set

$$I_+(x) := \{i \in [d] \mid \lambda_i > 0\} \qquad \text{and} \qquad I_-(x) := \{i \in [d] \mid \lambda_i < 0\}.$$

b) If $x \in \mathbb{R}^d$ is generic with respect to $C_{\mathcal{B}}$ then we define the following half-open sets.
   i) The near half-open cone
$$C_{\mathcal{B}}[x] := \left\{ \sum_{i\in[d]} \mu_i v_i \;\middle|\; \begin{smallmatrix} \mu_i>0 \text{ if } i\in I_+(x) \\ \mu_i\geq 0 \text{ if } i\in I_-(x) \end{smallmatrix} \right\}$$
   ii) The near half-open parallelepiped
$$\mathsf{Epi}_{\mathcal{B}}[x] := \left\{ \sum_{i\in[d]} \mu_i v_i \;\middle|\; \begin{smallmatrix} \mu_i\in(0,1] \text{ if } i\in I_+(x) \\ \mu_i\in[0,1) \text{ if } i\in I_-(x) \end{smallmatrix} \right\}$$
   iii) The far half-open cone
$$C_{\mathcal{B}}(x] := \left\{ \sum_{i\in[d]} \mu_i v_i \;\middle|\; \begin{smallmatrix} \mu_i\geq 0 \text{ if } i\in I_+(x) \\ \mu_i>0 \text{ if } i\in I_-(x) \end{smallmatrix} \right\}$$
   iv) The far half-open parallelepiped
$$\mathsf{Epi}_{\mathcal{B}}(x] := \left\{ \sum_{i\in[d]} \mu_i v_i \;\middle|\; \begin{smallmatrix} \mu_i\in[0,1) \text{ if } i\in I_+(x) \\ \mu_i\in(0,1] \text{ if } i\in I_-(x) \end{smallmatrix} \right\}$$

The next lemma generalizes Lemma 2.5 to the near and far half-open parallelepipeds $\mathsf{Epi}_{\mathcal{B}}[x)$ and $\mathsf{Epi}_{\mathcal{B}}(x]$ and shows that they can be used to tile $\mathbb{R}^d$. We state the next lemma for $\mathsf{Epi}_{\mathcal{B}}[x)$ only but the proof easily translates to $\mathsf{Epi}_{\mathcal{B}}(x]$.

Lemma 5.6.
For a linearly independent set $\mathcal{B} = \{v_1, \dots, v_d\} \subset \mathbb{R}^d$, consider the cone $C_{\mathcal{B}} := \mathsf{cone}(B)$ and the lattice $\Lambda_{\mathcal{B}}$ and let $x \in \mathbb{R}^d$ be generic with respect to $C_{\mathcal{B}}$. Then every $z \in \mathbb{R}^d$ has a unique representation $z = v + y$ where $v \in \Lambda_{\mathcal{B}}$ and $y \in \mathsf{Epi}_{\mathcal{B}}[x)$.

Proof. For $x, z \in \mathbb{R}^d$ with x generic for $C_{\mathcal{B}}$, consider their expansions with respect to $\mathcal{B}$:

$$x = \sum_{i\in[d]} \lambda_i v_i \qquad \text{and} \qquad z = \sum_{i\in[d]} \mu_i v_i.$$

Now define

$$v := \sum_{i\in I_+(x)} \lfloor \mu_i \rfloor v_i + \sum_{i\in I_i(x)} (\lceil \mu_i \rceil - 1)\, v_i \qquad \text{and} \qquad y := z - v.$$

Then $v \in \Lambda_{\mathcal{B}}$ and $z = v + y$. It remains to show that $y \in \mathsf{Epi}_{\mathcal{B}}[x)$. Since

$$y = \sum_{i\in I_+(x)} (\mu_i - \lfloor \mu_i \rfloor)\, v_i + \sum_{i\in I_-(x)} (\mu_i - \lceil \mu_i \rceil + 1)\, v_i$$

where $(\mu_i - \lfloor \mu_i \rfloor) \in [0,1)$ and $(\mu_i - \lceil \mu_i \rceil + 1) \in (0,1]$, we conclude that $y \in \mathsf{Epi}_{\mathcal{B}}[x)$.

To show uniqueness, assume $z = v + y = \widetilde{v} + \widetilde{y}$ with $v, \widetilde{v} \in \Lambda_{\mathcal{B}}$ and $y, \widetilde{y} \in \mathsf{Epi}_{\mathcal{B}}[x)$. Then

$$y = \sum_{i \in [d]} \alpha_i v_i \qquad \text{and} \qquad \widetilde{y} = \sum_{i \in [d]} \widetilde{\alpha}_i v_i$$

where $\alpha_i, \widetilde{\alpha}_i \in (0,1]$ if $i \in I_+(x)$ and $\alpha_i, \widetilde{\alpha}_i \in [0,1)$ if $i \in I_-(x)$. This implies $|\alpha_i - \widetilde{\alpha}_i| < 1$ for all $i \in [d]$. From $\widetilde{y} - y = v - \widetilde{v} \in \Lambda_{\mathcal{B}}$ we conclude $\alpha_i - \widetilde{\alpha}_i \in \mathbb{Z}$which in turn implies $\alpha_i = \widetilde{\alpha}_i$ for all $i \in [d]$. This shows $\widetilde{y} = y$ and $v = \widetilde{v}$ as claimed. □

This lemma not only allows to decompose $\mathbb{R}^d$ into Λ-translates of half-open parallelepipeds but also to decompose the near and far half-open cones $C_{\mathcal{B}}[x)$ and $C_{\mathcal{B}}(x]$ into disjoint unions of Λ-translates of $\mathsf{Epi}_{\mathcal{B}}[x)$ and $\mathsf{Epi}_{\mathcal{B}}(x]$.

Corollary 5.7. *With the same assumptions as for Lemma 5.6, we have*

$$C_{\mathcal{B}}[x) = \bigsqcup_{v \in \mathsf{span}_{\mathbb{N}_0}\mathcal{B}} (\mathsf{Epi}_{\mathcal{B}}[x) + v) \qquad \text{and} \qquad C_{\mathcal{B}}(x] = \bigsqcup_{v \in \mathsf{span}_{\mathbb{N}_0}\mathcal{B}} (\mathsf{Epi}_{\mathcal{B}}(x] + v)\,.$$

Proof. The previous Lemma 5.6 shows that $\mathbb{R}^d$ is the disjoint union of $\Lambda_{\mathcal{B}}$-translates of $\mathsf{Epi}_{\mathcal{B}}[x)$. It remains to observe that

$$C_{\mathcal{B}}[x) \cap (\mathsf{Epi}_{\mathcal{B}}[x) + v) = \begin{cases} (\mathsf{Epi}_{\mathcal{B}}[x) + v) & \text{if } v \in \mathsf{span}_{\mathbb{N}_0}\mathcal{B}, \\ \varnothing & \text{if } v \in \Lambda_{\mathcal{B}} \setminus \mathsf{span}_{\mathbb{N}_0}\mathcal{B}. \end{cases}$$

The proof for the second statement is similar. □

Definition 5.8 (subdivisions, triangulations)**.**
Let P denote a polytope or a polyhedral cone.
a) A subdivision of P is a polyhedral complex $\mathcal{C}$ such that $P = \bigcup_{F \in \mathcal{C}} F$.
b) A subdivision $\mathcal{T}$ of P is a triangulation of P if all cells are simplices (if P is a polytope) or simplicial cones (if P is a polyhedral cone).
c) A triangulation $\mathcal{T}$ of a polytope P of dimension d is without new vertices (or: has no new vertices) if $\mathsf{vert}(\sigma) \subseteq \mathsf{vert}(P)$ for all $\sigma \in \mathcal{T}_d$. A triangulation $\mathcal{T}$ of a polyhedral cone of dimension d and generated by $V = \{v_1, \ldots, v_r\}$ is without new vertices (or has no new vertices) if every simplicial cone $\sigma \in \mathcal{T}_d$ is generated by a subset of V

Notice that every polytope $P = \mathsf{conv}\{v_1, \ldots, v_r\}$ and every polyhedral cone $P = \mathsf{cone}\{v_1, \ldots, v_r\}$ has a triangulation $\mathcal{T}$ without new vertices. Given a triangulation of a cone or polytope, we now aim to decompose it into disjoint half-open simplices or cones (Proposition 5.10). We need the following auxiliary Lemma 5.9. It is straight-forward to extend the statement to the situation where $\mathcal{B} = \{v_1, \ldots, v_r\} \subset \mathbb{R}^d$ is linearly independent and $r < d$.

Lemma 5.9.
Let $x_0 \in \mathbb{R}^d$ be generic with respect to the polyhedral cone $C_{\mathcal{B}} = \mathsf{cone}(\mathcal{B})$ with $\mathcal{B} = \{v_1, \ldots, v_d\} \subset \mathbb{R}^d$ linearly independent. We define

$$y_\varepsilon := (1-\varepsilon)y + \varepsilon x_0$$

for $y \in \mathbb{R}^d$ and $\varepsilon > 0$. Then
a) $y \in C_{\mathcal{B}}[x_0) \iff \exists\, \delta > 0 \quad \forall\, 0 < \varepsilon < \delta : \quad y_\varepsilon \in \operatorname{int}(C_{\mathcal{B}})$.
b) $y \in C_{\mathcal{B}}(x_0] \iff \exists\, \delta > 0 \quad \forall\, 0 < \varepsilon < \delta : \quad y_{-\varepsilon} \in \operatorname{int}(C_{\mathcal{B}})$.

Proof. If $x_0, y \in \mathbb{R}^d$ with x_0 generic with respect to $C_{\mathcal{B}}$ then $x_0 = \sum_{i \in [d]} \lambda_i v_i$ and $y = \sum_{i \in [d]} \mu_i v_i$ where $\lambda_i \in \mathbb{R} \setminus \{0\}$ and $\mu_i \in \mathbb{R}$ for $i \in [d]$. Thus $y_\varepsilon = \sum_{i \in [d]} \left((1-\varepsilon)\mu_i + \varepsilon\lambda_i\right) v_i$ and we conclude that there exists $\delta > 0$ such that $(1-\varepsilon)\mu_i + \varepsilon\lambda_i > 0$ for all $0 < \varepsilon < \delta$ if and only if either i) $\mu_i > 0$ or ii) $\mu_i = 0$ and $\lambda_i > 0$. This implies the first claim.

The second claim is proven similarly using that $(1+\varepsilon)\mu_i - \varepsilon\lambda_i > 0$ if and only if either i) $\mu_i > 0$ or ii) $\mu_i = 0$ and $\lambda_i < 0$. □

Proposition 5.10.
Let $\mathcal{T}$ be a triangulation of a cone $C = \mathsf{cone}(\mathcal{B}) \subset \mathbb{R}^d$ with $\dim(\mathsf{span}_{\mathbb{R}}\mathcal{B}) = d$. If $x_0 \in C$ is generic with respect to every $\sigma \in \mathcal{T}_d$ then

$$C = \bigsqcup_{\sigma\in\mathcal{T}_d} \sigma(x_0] \qquad \text{and} \qquad \operatorname{int}(C) = \bigsqcup_{\sigma\in\mathcal{T}_d} \sigma[x_0).$$

Proof. First, $x_0 \in C$ implies that $y \in C$ if and only if $0 \le \varepsilon \le 1$ that $y_\varepsilon := (1-\varepsilon)y + \varepsilon x_0 \in C$. Since $\mathcal{T}$ is a triangulation of C and x_0 is generic with respect to every $\sigma \in \mathcal{T}_d$, we conclude that there exist $\delta > 0$ and a unique $\sigma \in \mathcal{T}_d$ such that $y_\varepsilon \in \operatorname{int}(\sigma)$ for all $0 < \varepsilon < \delta$. Now part a) of Lemma 5.9 implies $y \in \sigma[x_0)$ as well as $y \notin \tau[x_0)$ for all $\tau \in \mathcal{T}_d \setminus \{\sigma\}$.

For the second claim, notice that x_0 is also generic with respect to C. This implies that $y \in \operatorname{int}(C)$ if and only if there is $\delta > 0$ such that $y_{-\varepsilon} := (1+\varepsilon)y - \varepsilon x_0 \in \operatorname{int}(C)$ for all $0 < \varepsilon < \delta$. Since $\mathcal{T}$ is a triangulation of C, we conclude that there is a unique simplicial cone $\sigma \in \mathcal{T}_d$ such that $y_{-\varepsilon} \in \sigma$ for $0 < \varepsilon < \delta$ and $\delta > 0$ sufficiently small. Now apply part b) of Lemma 5.9. □

5.2. **Encoding points of cones via generating functions.**
How could we encode the lattice points of the line segment $P = [0, b] \subset \mathbb{R}$ for $b \ge 0$? The naive approach simply lists all points: 0, 1, 2, …, b. A more sophisticated way is to use a polynomials or formal power series and to consider

$$\textstyle\sum_{i=0}^{b} t^i = \sum_{a\in P\cap\mathbb{Z}} t^a.$$

This is a relatively efficient way to encode even infinitely many points and the number of points is retrieved by evaluating this polynomial at $t = 1$. Notice that we can go a step further since

$$\textstyle\sum_{i=0}^{b} t^i = \frac{1-t^{b+1}}{1-t}.$$

Although this rational function has a singularity which prevents us to evaluate this function at $t = 1$, this correspondence has the advantage that it 'extends to infinity': $\sum_{i\in\mathbb{N}_0} t^i = \frac{1}{1-t}$.

This encoding can be extended from 1-dimensional line segments to higher dimensional polytopes $P \subset \mathbb{R}^d$: consider polynomials in more than one variable where each point $\boldsymbol{a} \in P \cap \mathbb{Z}^d$ corresponds to a monomial:

$$\boldsymbol{a} = (a_1, a_2, \ldots, a_d) \in P \cap \mathbb{Z}^d \quad \longmapsto \quad \boldsymbol{t^a} := \textstyle\prod_{i\in[d]} t_i^{a_i}$$

while the entire set $P \cap \mathbb{Z}^d$ corresponds to

$$P \cap \mathbb{Z}^d \quad \longmapsto \quad \textstyle\sum_{\boldsymbol{a}\in P\cap\mathbb{Z}^d} \left(\prod_{i\in[d]} t_i^{a_i}\right) = \sum_{\boldsymbol{a}\in P\cap\mathbb{Z}^d} \boldsymbol{t^a}.$$

We may encounter some technical problems. First, if $a_i < 0$ then we do not obtain a polynomial. Second, $P \cap \mathbb{Z}^d$ can be unbounded. The first issue is resolved if we consider Laurent polynomials instead of polynomials. The set of Laurent polynomials is defined as

$$\mathsf{L} := \mathbb{R}[t_1, t_1^{-1}, t_2, t_2^{-1}, \ldots, t_d, t_d^{-1}],$$

that is, L consists of all polynomials in the $2d$ variables t_i and t_i^{-1} for $i \in [d]$. Both problems are resolved by allowing formal Laurent series

$$\widehat{\mathsf{L}} = \mathbb{R}[\![t_1, t_1^{-1}, t_2, t_2^{-1}, \ldots, t_d, t_d^{-1}]\!],$$

that is, formal power series in these $2d$ variables. Notice that Laurent polynomials and series form abelian groups with respect to addition:

$$\textstyle\sum_{\boldsymbol{a}\in\mathbb{Z}^d} \lambda_{\boldsymbol{a}}\boldsymbol{t^a} + \sum_{\boldsymbol{a}\in\mathbb{Z}^d} \mu_{\boldsymbol{a}}\boldsymbol{t^a} = \sum_{\boldsymbol{a}\in\mathbb{Z}^d} (\lambda_{\boldsymbol{a}} + \mu_{\boldsymbol{a}})\boldsymbol{t^a}.$$

Moreover, the multiplication

$$\left(\textstyle\sum_{\boldsymbol{a}\in\mathbb{Z}^d} \lambda_{\boldsymbol{a}}\boldsymbol{t^a}\right) \cdot \left(\sum_{\boldsymbol{a}\in\mathbb{Z}^d} \mu_{\boldsymbol{a}}\boldsymbol{t^a}\right) = \sum_{\boldsymbol{a}\in\mathbb{Z}^d} \left(\sum_{\boldsymbol{b}\in\mathbb{Z}^d} \lambda_{\boldsymbol{a}-\boldsymbol{b}}\mu_{\boldsymbol{b}}\right) \cdot \boldsymbol{t^a}$$

turns L into a commutative ring and $\widehat{\mathsf{L}}$ into an L-module.

Example 5.11. The polygon $P := \mathsf{conv}\left\{\binom{0}{1}, \binom{2}{-1}, \binom{2}{2}, \binom{3}{0}\right\}$ has associated Laurent polynomial

$$t_1^2t_2^2 + t_2 + t_1t_2 + t_1^2t_2 + t_1 + t_1^2 + t_1^3 + t_1^2t_2^{-1}.$$

Definition 5.12 (integer point series, summable Laurent series)**.**
a) For $S \subseteq \mathbb{R}^d$, we define the integer point series $\widehat{\mathsf{G}}_S(\boldsymbol{t})$ as the formal Laurent series

$$\widehat{\mathsf{G}}_S(\boldsymbol{t}) := \textstyle\sum_{a\in S\cap\mathbb{Z}^d} \boldsymbol{t}^a \in \widehat{\mathsf{L}}.$$

b) A Laurent series $\widehat{\mathsf{G}}(\boldsymbol{t}) \in \widehat{\mathsf{L}}$ is summable if $g \cdot \widehat{\mathsf{G}} \in \mathsf{L}$ for some (non-vanishing) $g \in \mathsf{L} \setminus \{0\}$. The set of all summable Laurent series of $\widehat{\mathsf{L}}$ is denoted by $\widehat{\mathsf{L}}^{sum}$

Remark 5.13.
a) Every Laurent polynomial is a summable Laurent series.
b) If $S \subseteq \mathbb{R}^d$ and $v \in R^d$ then the translate of S by v is $S + v = \{s + v \mid s \in S\} \subseteq \mathbb{R}^d$. Then

$$\widehat{\mathsf{G}}_{S+v}(\boldsymbol{t}) = \boldsymbol{t}^v \cdot \widehat{\mathsf{G}}_S(\boldsymbol{t}).$$

The proof of the next proposition is left as exercise.

Proposition 5.14.
$\widehat{\mathsf{L}}^{sum}$ is an L-submodule of $\widehat{\mathsf{L}}$.

Example 5.15.
a) The ray $P_\infty = [0, \infty]$.
As previously discussed, we have $\widehat{\mathsf{G}}_{P_\infty}(t) = \sum_{i\in\mathbb{N}_0} t^i \in \widehat{\mathsf{L}}$ as well as $g(t) \cdot \widehat{\mathsf{G}}_{P_\infty}(t) = 1 \in \mathsf{L}$ for $g(t) = 1 - t \in \mathsf{L}$. This shows that $\widehat{\mathsf{G}}_{P_\infty}(t) \in \widehat{\mathsf{L}}^{sum}$.
b) The cone $C = \mathsf{cone}\{e_1, e_2\}$.
We have $\widehat{\mathsf{G}}_C(t_1, t_2) = \sum_{a,b\in\mathbb{N}_0} t_1^a t_2^b \in \widehat{\mathsf{L}}$. Moreover, we have $g(t_1, t_2) \cdot \widehat{\mathsf{G}}_C(t_1, t_2) = 1 \in \mathsf{L}$ for $g(t_1, t_2) = (1 - t_1)(1 - t_2) \in \mathsf{L}$. This shows that $\widehat{\mathsf{G}}_C(t_1, t_2) \in \widehat{\mathsf{L}}^{sum}$.
c) The simplicial cone $C = \mathsf{cone}(\mathcal{B})$ generated by $\mathcal{B} = \{v_1, \ldots, v_d\} \subset \mathbb{Z}^d$.
We have $\widehat{\mathsf{G}}_C(\boldsymbol{t}) = \sum_{a\in C\cap\mathbb{Z}^d} \boldsymbol{t}^a$ and claim that $\widehat{\mathsf{G}}_C(\boldsymbol{t}) \in \widehat{\mathsf{L}}^{sum}$. To this respect, we notice

$$\prod_{i\in[d]} (1 - \boldsymbol{t}^{v_i}) \cdot \sum_{z\in\mathsf{span}_{\mathbb{N}_0}\mathcal{B}} \boldsymbol{t}^z = 1.$$

Moreover, if $x_0 \in C$ is generic with respect to C then $x \in C \cap \mathbb{Z}^d$ if and only if there exist unique $y \in \mathsf{Epi}_{\mathcal{B}}(x_0] \cap \mathbb{Z}^d$ and $z \in \mathsf{span}_{\mathbb{N}_0}\mathcal{B}$ with $x = y + z$. This implies

$$\begin{aligned}
\prod_{i\in[d]} (1 - \boldsymbol{t}^{v_i}) \cdot \widehat{\mathsf{G}}_C(\boldsymbol{t}) &= \prod_{i\in[d]} (1 - \boldsymbol{t}^{v_i}) \cdot \sum_{z\in C\cap\mathbb{Z}^d} \boldsymbol{t}^z \\
&= \prod_{i\in[d]} (1 - \boldsymbol{t}^{v_i}) \cdot \sum_{y\in\mathsf{Epi}_{\mathcal{B}}(x_0]\cap\mathbb{Z}^d} \; \sum_{z\in\mathsf{span}_{\mathbb{N}_0}\mathcal{B}} \boldsymbol{t}^{y+z} \\
&= \prod_{i\in[d]} (1 - \boldsymbol{t}^{v_i}) \cdot \sum_{y\in\mathsf{Epi}_{\mathcal{B}}(x_0]\cap\mathbb{Z}^d} \boldsymbol{t}^y \cdot \sum_{z\in\mathsf{span}_{\mathbb{N}_0}\mathcal{B}} \boldsymbol{t}^z \\
&= \sum_{y\in\mathsf{Epi}_{\mathcal{B}}(x_0]\cap\mathbb{Z}^d} \boldsymbol{t}^y
\end{aligned}$$

which shows that $\widehat{\mathsf{G}}_C(\boldsymbol{t}) \in \widehat{\mathsf{L}}^{sum}$.

Recall that a rational function can be seen as a quotient $\frac{p(\boldsymbol{t})}{q(\boldsymbol{t})}$ of polynomials $p, q \in \mathbb{R}[t_1, \ldots, t_d]$ where $q \neq 0$. We mimic the construction of rational numbers from integers and define an equivalence relation $\sim$ on these quotients via $\frac{p_1(\boldsymbol{t})}{q_1(\boldsymbol{t})} \sim \frac{p_2(\boldsymbol{t})}{q_2(\boldsymbol{t})}$ if and only if $p_1(\boldsymbol{t}) \cdot q_2(\boldsymbol{t}) = p_2(\boldsymbol{t}) \cdot q_1(\boldsymbol{t})$. This yields the field of rational functions $\mathbb{R}(t_1, \ldots, t_d)$ as set of equivalence classes $\left[\frac{p(\boldsymbol{t})}{q(\boldsymbol{t})}\right]$. Clearly, every Laurent polynomial can be identified with a rational function. Using implicitly this identification, we have $\mathsf{L} \subset \mathbb{R}(t_1, \ldots, t_d)$. In particular, the rational functions can be seen as an L-module. We

now relate summable Laurent series to rational functions and define

$$\Phi : \widehat{\mathsf{L}}^{sum} \longrightarrow \mathbb{R}(t_1, \ldots, t_d)$$
$$\widehat{\mathsf{G}}(\boldsymbol{t}) \longmapsto \left[\frac{p(\boldsymbol{t})}{q(\boldsymbol{t})}\right]$$

where $p(\boldsymbol{t}), q(\boldsymbol{t}) \in \mathsf{L}$ with $q(\boldsymbol{t}) \neq 0$ such that $q(\boldsymbol{t}) \cdot \widehat{\mathsf{G}}(\boldsymbol{t}) = p(\boldsymbol{t})$.

Proposition 5.16. *The map $\Phi : \widehat{\mathsf{L}}^{sum} \longrightarrow \mathbb{R}(t_1, \ldots, t_d)$ is well-defined and a homomorphism of L-modules.*

Proof. Exercise. □

Remark 5.17. As $\mathsf{L} \subset \widehat{\mathsf{L}}^{sum}$, we may consider L as an L-submodule of $\widehat{\mathsf{L}}^{sum}$. Similarly, L can be seen as an L-submodule of $\mathbb{R}(t_1, \ldots, t_d)$. As a consequence, restricting the homomorphism Φ to L yields the identity map: $\Phi_{|\mathsf{L}} = \mathsf{Id} : \mathsf{L} \to \mathsf{L}$.

Definition 5.18 (integer point generating function)**.**
If $S \subseteq \mathbb{R}^d$ such that $\widehat{\mathsf{G}}_S(\boldsymbol{t}) \in \widehat{\mathsf{L}}^{sum}$ then define the integer point generating function $\mathsf{G}_S(\boldsymbol{t})$ as

$$\mathsf{G}_S(\boldsymbol{t}) := \Phi\left(\widehat{\mathsf{G}}_S(\boldsymbol{t})\right) \in \mathbb{R}(t_1, \ldots, t_d).$$

Example 5.19.
a) A bounded set $S \subset \mathbb{R}^d$.
If $S \subset \mathbb{R}^d$ is bounded then $\mathsf{G}_S(1, \ldots, 1)$ yields the number of integer points in S. Details are left as exercise (compute the integer point generating function!).
b) The ray $P_\infty = [0, \infty] \subset \mathbb{R}$.
We have seen that $(1-t) \cdot \widehat{\mathsf{G}}_{P_\infty}(t) = 1$, so the integer point generating function is defined. We conclude that $\mathsf{G}_{P_\infty}(t) = \frac{1}{1-t}$. Notice that $\lim_{t\to 1} \frac{1}{1-t} = \infty$, so $\mathsf{G}_{P_\infty}(1)$ still counts (in a weak sense) the number of integer points in P_∞.

We now summarize our results on rational cones.

Theorem 5.20.
Let $\mathcal{B} = \{v_1, \ldots, v_d\} \subset \mathbb{Z}^d$ be a basis of $\mathbb{R}^d$ and $x_0 \in \mathbb{R}^d$ be generic with respect to the simplicial cone $C := \mathsf{cone}(\mathcal{B})$. Then
a) The integer point series $\widehat{\mathsf{G}}_{C_{\mathcal{B}}[x_0)}(\boldsymbol{t})$ of the half-open cone $C_{\mathcal{B}}[x_0)$ is a summable Laurent series.
b) The integer point generating function $\mathsf{G}_{C_{\mathcal{B}}[x_0)}(\boldsymbol{t})$ of the half-open cone $C_{\mathcal{B}}[x_0)$ satisfies

$$\mathsf{G}_{C_{\mathcal{B}}[x_0)}(\boldsymbol{t}) = \frac{\mathsf{G}_{\mathsf{Epi}_{\mathcal{B}}(x_0]}(\boldsymbol{t})}{\prod_{i\in[d]}(1-\boldsymbol{t}^{v_i})} \in \mathbb{R}(t_1, \ldots, t_d).$$

Proof. Consider the sub-lattice $\Gamma := \Gamma_{\mathcal{B}}$ of the standard integer lattice $\Lambda = \mathbb{Z}^d$. Then $x \in C_{\mathcal{B}}[x_0)$ if and only if there are a unique $y \in \mathsf{Epi}_{\mathcal{B}}(x_0]$ and $z \in \Gamma \cap \mathbb{Z}^d$ such that $x = y + z$. For the integer point series of the half-open cone $C_{\mathcal{B}}[x_0)$, this implies

$$\begin{aligned}
\widehat{\mathsf{G}}_{C_{\mathcal{B}}[x_0)}(\boldsymbol{t}) &= \sum_{z\in C_{\mathcal{B}}[x_0)\cap\mathbb{Z}^d} \boldsymbol{t}^{y+z} \\
&= \sum_{y\in \mathsf{Epi}_{\mathcal{B}}(x_0]\cap\mathbb{Z}^d} \; \sum_{z\in \mathsf{span}_{\mathbb{N}_0}\mathcal{B}} \boldsymbol{t}^{y+z} \\
&= \sum_{y\in \mathsf{Epi}_{\mathcal{B}}(x_0]\cap\mathbb{Z}^d} \boldsymbol{t}^{y} \sum_{z\in \mathsf{span}_{\mathbb{N}_0}\mathcal{B}} \boldsymbol{t}^{z}.
\end{aligned}$$

Adapting the argument of Example 5.15 c) to half-open cones proves $\widehat{\mathsf{G}}_{C_{\mathcal{B}}[x_0)}(\boldsymbol{t}) \in \widehat{\mathsf{L}}^{sum}$ and the first claim. Application of the homomorphism Φ yields the second claim. □

Corollary 5.21. *Let $C := \mathsf{cone}(\mathcal{B})$ be the simplicial cone generated by a linearly independent set $\mathcal{B} = \{v_1, \ldots, v_d\} \subset \mathbb{Z}^d$ and let $x_0 \in C$ be generic with respect to C. Then*

$$\mathsf{G}_C(\boldsymbol{t}) = \frac{\mathsf{G}_{\mathsf{Epi}_{\mathcal{B}}(x_0]}(\boldsymbol{t})}{\prod_{i\in[d]}(1-\boldsymbol{t}^{v_i})}.$$

Corollary 5.22. *Let $C := \mathsf{cone}(\mathcal{V})$ be the cone generated by $\mathcal{V} = \{v_1, \ldots, v_r\} \subset \mathbb{Z}^d$ with $\dim(\mathsf{span}_{\mathbb{R}}(\mathcal{V})) = d$, let $\mathcal{T}$ be a triangulation of C and $x_0 \in C$ be generic with respect to C. Then*

$$\widehat{\mathsf{G}}_C(\boldsymbol{t}) = \sum_{\sigma\in\mathcal{T}_d} \widehat{\mathsf{G}}_{\sigma(x_0]}(\boldsymbol{t}) \qquad \text{and} \qquad \widehat{\mathsf{G}}_{\mathrm{int}(C)}(\boldsymbol{t}) = \sum_{\sigma\in\mathcal{T}_d} \widehat{\mathsf{G}}_{\sigma[x_0)}(\boldsymbol{t}).$$

Remark 5.23.

a) Clearly, Corollary 5.22 could also be phrased in terms of the integer point generating function instead of the integer point series.

b) Notice that the denominator of the integer point generating function of a simplicial rational cone C is determined by a set of generators of C. Therefore, the difficult part in computing the integer point generating function is to determine the integer points of $\mathsf{Epi}_{\mathcal{B}}(x_0]$ or, equivalently, the computation of its integer point generating function.

6. Erhart theory: counting lattice points of polytopes

6.1. **The Ehrhart polynomial of a lattice polytope.**

To simplify the presentation, we restrict to the situation where $\Lambda = \mathbb{Z}^d \subset \mathbb{R}^d$ is the standard integer lattice in $\mathbb{R}^d$. If $P \subset \mathbb{R}^d$ is a d-dimensional polytope with vertex set $\mathsf{ver}(P) = \{v_1, \ldots, v_r\} \subset \mathbb{Z}^d$ then we again embed P in $\mathbb{R}^{d+1}$ to obtain $\widetilde{P}$ with vertex set $\mathsf{ver}(\widetilde{P}) = \{\binom{v_1}{1}, \ldots, \binom{v_r}{1}\} \subset \mathbb{Z}^{d+1}$. Clearly, P and $\widetilde{P}$ contain the same number of integer points and $C := \mathsf{cone}(\mathsf{ver}(\widetilde{P})) \subset \mathbb{R}^{d+1}$ is a polyhedral cone. Moreover:

a) Any dilate $k\widetilde{P}$ (by a positive integer k) can be recovered from C by intersecting C with the hyperplane $\{x \in \mathbb{R}^{d+1} \mid x_{d+1} = k\}$.
b) Every point of $C \cap \mathbb{Z}^{d+1}$ is a lattice point of precisely one dilate $k\widetilde{P}$ and the number of integer points of kP coincides with the number of integer points of $k\widetilde{P}$.
c) Any triangulation $\mathcal{T}$ without new vertices of P induces a triangulation $\widetilde{\mathcal{T}}$ of C.

If we write $(\boldsymbol{s}, t) \in \mathbb{R}^d \times \mathbb{R}$ then the integer point series of C evaluated at $\boldsymbol{s} = (1, \ldots, 1)$ yields

$$\widehat{\mathsf{G}}_C(1, \ldots, 1, t) = 1 + \sum_{k \in \mathbb{N}} |kP \cap \mathbb{Z}^d| \cdot t^k = 1 + \sum_{k \in \mathbb{N}} \mathsf{ehr}_P(k) \cdot t^k.$$

In particular, the integer point series $\widehat{\mathsf{G}}_C(t) := \widehat{\mathsf{G}}_C(1, \ldots, 1, t)$ is summable. This justifies the following definition.

Definition 6.1.
Let $P \subset \mathbb{R}^d$ be a d-dimensional polytope with $\mathsf{ver}(P) \subset \mathbb{Z}^d$. The Ehrhart series of P is defined as

$$\widehat{\mathsf{Ehr}}_P(t) := 1 + \sum_{k \in \mathbb{N}} \mathsf{ehr}_P(k) \cdot t^k \in \widehat{\mathsf{L}}^{sum}.$$

The corresponding rational generating function $\Phi\left(\widehat{\mathsf{Ehr}}_P(t)\right)$ is the rational function denoted by $\mathsf{Ehr}_P(t)$.

Proposition 6.2.
Let $P \subset \mathbb{R}^d$ be a d-dimensional lattice polytope, $C := \mathsf{cone}(\mathsf{ver}(\widetilde{P})) \subset \mathbb{R}^{d+1}$ be the induced cone, $\mathcal{T}$ be a triangulation of C which is induced by a lattice triangulation of P and $x_0 \in C$ be generic with respect to all $\sigma \in \mathcal{T}_{d+1}$. Then

$$\mathsf{Ehr}_P(t) = \frac{\sum_{\sigma \in \mathcal{T}_{d+1}} \mathsf{G}_{\mathsf{Epi}_{\widetilde{V}}(x_0)}(1, \ldots, 1, t)}{(1-t)^{d+1}}.$$

Proof. The claim is an immediate consequence of $\mathsf{Ehr}_P(t) = \mathsf{G}_C(1, \ldots, 1, t)$ and the linearity of Φ. □

Our next goal is to prove that the Ehrhart counting function $\mathsf{ehr}_P : \mathbb{N} \to \mathbb{R}$ extends uniquely to a polynomial $\mathsf{ehr}_P : \mathbb{R} \to \mathbb{R}$. We need the following properties of the Ehrhart series of a simplex and a general result on generating functions.

Proposition 6.3.
Let $P \subset \mathbb{R}^d$ be a lattice d-simplex with vertex set $\mathsf{ver}(P) = \{v_1, \ldots, v_{d+1}\} \subset \mathbb{Z}^d$. Then

$$\mathsf{Ehr}_P(t) = \frac{h^*(t)}{(1-t)^{d+1}}$$

where $h^*(t) \in \mathbb{R}[t]$ with $\deg(h^*) \leq d$ and $h^*(1) \neq 0$.

In particular, if $h^*(t) = \sum_{k=0}^{d} h_k^* t^k$ and $\widetilde{V} = \{\binom{v_1}{1}, \ldots, \binom{v_{d+1}}{1}\}$ then

$$h_k^* = \left|\mathsf{Epi}_{\widetilde{V}}(x_0] \cap \mathbb{Z}^{d+1} \cap \{x \in \mathbb{R}^{d+1} \mid x_{d+1} = k\}\right|$$

for $x_0 \in \mathrm{int}(\mathsf{cone}(\widetilde{V}))$

Proof. The vertex set $\widetilde{V} = \mathsf{ver}(\widetilde{P}) \subset \mathbb{R}^{d+1}$ is linearly independent since P is a d-simplex. The cone $C = \mathsf{cone}(\widetilde{V})$ is therefore simplicial and we consider the sublattice $\Gamma := \Gamma_{\widetilde{V}}$ of $\Lambda = \mathbb{Z}^d$ together with the associated fundamental domain $\Pi := \Pi_{\widetilde{V}}$. Proposition 6.2 implies

$$\mathsf{Ehr}_P(t) = \frac{\mathsf{G}_{\mathsf{Epi}_{\widetilde{V}}(x_0]}(1,\ldots,1,t)}{(1-t)^{d+1}}$$

for some $x_0 \in C$ that is generic with respect to C. Since $\widehat{\mathsf{G}}_{\mathsf{Epi}_{\widetilde{V}}(x_0]}(\boldsymbol{s},t) = \widehat{\mathsf{G}}_{\Pi}(\boldsymbol{s},t)$, we conclude that $h^*(t)$ is the Laurent polynomial $\mathsf{G}_{\Pi}(1,\ldots,1,t)$ which is in particular a rational function. Since $\widehat{\mathsf{G}}_{\Pi}(\boldsymbol{s},t) = \sum_{(\boldsymbol{a},b)\in\Pi\cap\mathbb{Z}^d} \boldsymbol{s}^{\boldsymbol{a}} t^b$ and since $\Pi \subset \mathbb{R}^{d+1}$ is a bounded set that is contained in $\left\{x \in \mathbb{R}^{d+1} \;\middle|\; x_{d+1} \geq 0\right\}$, we obtain that $h^*(t)$ is in fact a polynomial and its degree $\deg(h^*(t))$ is $\leq d$ since $x \in \Pi$ if and only if $x = \sum_{i\in[d+1]} \lambda_i \binom{v_i}{1}$ with $0 \leq \lambda_i < 1$. To see that $h^*(1) \neq 0$, notice that

$$\widehat{\mathsf{G}}_{\Pi}(1,\ldots,1,1) = \left|\Pi \cap \mathbb{Z}^{d+1}\right| > 0$$

since $0 \in \Pi$. The last claim, that is,

$$h_k^* = \left|\mathsf{Epi}_{\widetilde{V}}(x_0] \cap \mathbb{Z}^{d+1} \cap \left\{x \in \mathbb{R}^{d+1} \;\middle|\; x_{d+1} = k\right\}\right|$$

is implied by the fact that $\boldsymbol{s}^{\boldsymbol{a}} t^b$ is a monomial of $\widehat{\mathsf{G}}_{\Pi}(\boldsymbol{s},t)$ if and only if $(\boldsymbol{a},b) \in \Pi \cap \mathbb{Z}^{d+1}$. □

Remark 6.4.
Proposition 6.3 extends to all half-open simplices $C_{\widetilde{V}}(x_0] \cap \left\{x \in \mathbb{R}^{d+1} \;\middle|\; x_{d+1} = 1\right\}$ for all $x_0 \in \mathbb{R}^{d-1}$ that are generic with respect to $C = \mathsf{cone}(\widetilde{V})$.

The next proposition is a general result on generating functions and the crucial ingredient of our proof that the Ehrhart counting function extends to a polynomial.

Proposition 6.5.
Let $f : \mathbb{N} \to \mathbb{R}$ and $g : \mathbb{R} \to \mathbb{R}$ be two functions such that $\sum_{i\in\mathbb{N}_0} f(t)z^t = \frac{g(z)}{(1-z)^{d+1}}$. Then the following two statements are equivalent:
a) $f(t)$ extends uniquely to a polynomial $f : \mathbb{R} \to \mathbb{R}$ of degree d.
b) $g(z) = \sum_{k=0}^{d} g_k z^k$ is a polynomial of degree at most d with $g_0 \neq 0$.
If one of the two statements is satisfied then $f(t) = \sum_{k=0}^{d} g_k \cdot \binom{t+d-k}{d}$.

Proof. For $k \in \mathbb{Z}$ and $0 \leq k \leq d$, consider the polynomials $f_k(t) := \binom{t+d-k}{d}$. Then $\{f_0(t),\ldots,f_d(t)\}$ is a basis of the vector space of polynomials of degree at most d.

First, suppose that $f(t) \in \mathbb{R}[t]$ with $\deg(f) \leq d$, that is, $f(t) = \sum_{k=0}^{d} \lambda_k f_k(t) = \sum_{k=0}^{d} \mu_k t^k$. Since $deg(f) = d$, we know that $0 \neq \mu_d = \frac{1}{d!}\sum_{k=0}^{d} \lambda_k$ and we conclude that not all λ_k vanish simultaneously. Moreover,

$$\begin{aligned}
\sum_{t\in\mathbb{N}_0} f(t)z^t &= \sum_{t\in\mathbb{N}_0}\sum_{j=0}^{d} \lambda_j f_j(t) z^t &&= \sum_{j=0}^{d} \lambda_j \sum_{t\in\mathbb{N}_0} \binom{t+d-j}{d} z^t \\
&= \sum_{j=0}^{d} \lambda_j \sum_{t=j}^{\infty} \binom{t+d-j}{d} z^t &&= \sum_{j=0}^{d} \lambda_j \sum_{\widetilde{t}=0}^{\infty} \binom{\widetilde{t}+d}{d} z^{\widetilde{t}+j} \\
&= \sum_{j=0}^{d} \lambda_j z^j \sum_{t\in\mathbb{N}_0} \binom{t+d}{d} z^t &&= \frac{\sum_{j=0}^{d} \lambda_j z^j}{(1-z)^{d+1}} \\
&= \frac{g(z)}{(1-t)^{d+1}}
\end{aligned}$$

where $g(z) = \sum_{k=0}^{d} \lambda_k z^k$. Thus a) implies b), the other implication is proved similarly. □

Theorem 6.6 (Ehrhart's Theorem)**.**
Let $P \subset \mathbb{R}^d$ be a d-dimensional lattice polytope. Then

$$\Phi\left(\widehat{\mathsf{Ehr}}_P(t)\right) = \Phi\left(1 + \sum_{k\in\mathbb{N}} \mathsf{ehr}_P(k)t^k\right) = \frac{h^*(t)}{(1-t)^{d+1}}$$

where $\mathsf{ehr}_P(t) \in \mathbb{R}[t]$ with $\deg(\mathsf{ehr}_P) = d$ and $h^*(t) \in \mathbb{Z}[t]$ with $\deg(h^*) \leq d$ and $h^*(0) \neq 0$.

For historical reasons, we separate the following corollary from Ehrhart's Theorem although we prove both claims together.

Corollary 6.7 (Stanley's Non-negativity Theorem)**.**
Let $P \subset \mathbb{R}^d$ be a d-dimensional lattice polytope with $\mathsf{Ehr}_P(t) = \frac{h^*(t)}{(1-t)^{d+1}}$ where $h^*(t) = \sum_{k=0}^d h_k^* t^k$. Then $h_1^* = \ldots = h_d^* \geq 0$ and $h_0^* = 1$.

Proof. Let $\mathcal{T}$ be a triangulation of $C = \mathsf{cone}(\mathsf{ver}(\widetilde{P}))$ without new vertices and let $x_0 \in C$ be generic with respect to all $\sigma \in \mathcal{T}_{d+1}$. Then

$$\begin{aligned}
\Phi\left(\widehat{\mathsf{Ehr}}_P(t)\right) &= \Phi\left(\widehat{G}_C(1,\ldots,1,t)\right) \\
&= \Phi\Big(\sum_{\sigma\in\mathcal{T}_{d+1}} \widehat{\mathsf{G}}_{\sigma(x_0]}(1,\ldots,1,t)\Big) \\
&= \sum_{\sigma\in\mathcal{T}_{d+1}} \frac{\mathsf{G}_{\mathsf{Epi}_\sigma(x_0]}(1,\ldots,1,t)}{(1-t)^{d+1}} \\
&= \sum_{\sigma\in\mathcal{T}_{d+1}} \frac{\sum_{\boldsymbol{a}\in\mathsf{Epi}_\sigma(x_0]\cap\mathbb{Z}^{d+1}} t^{a_{d+1}}}{(1-t)^{d+1}}
\end{aligned}$$

As $0 \leq x_{d+1} < d+1$ for all points $x \in \mathsf{Epi}_\sigma(x_0]$, we conclude that

$$h^*(t) = \textstyle\sum_{\sigma\in\mathcal{T}_{d+1}} \sum_{\boldsymbol{a}\in\mathsf{Epi}_\sigma(x_0]\cap\mathbb{Z}^{d+1}} t^{a_{d+1}}$$

is a polynomial with integer coefficients of degree at most d. Moreover, $0 \in \mathsf{Epi}_\sigma(x_0]$ for precisely one $\sigma \in \mathcal{T}_{d+1}$, so $h_0^* = 1 \neq 0$. The coefficients h_k^* count the integer points x of $\mathsf{Epi}_\sigma(x_0]$ with $x_{d+1} = k$, so $h_k^* \geq 0$. If we consider the half-open polytopes

$$P_\sigma(x_0] := C_\sigma(x_0] \cap \left\{x \in \mathbb{R}^{d+1} \;\middle|\; x_{d_1} = 1\right\} \quad \text{with} \quad \widehat{\mathsf{Ehr}}_{P_\sigma(x_0]}(t) = 1 + \textstyle\sum_{k\in\mathbb{N}} \mathsf{ehr}_{P_\sigma(x_0]}(k)\cdot t^k$$

for all $\sigma \in \mathcal{T}_{d_1}$ then $\sum_{\sigma\in\mathcal{T}_{d+1}} \widehat{\mathsf{Ehr}}_{P_\sigma(x_0](t)} = \widehat{\mathsf{Ehr}}_P(t)$ and Proposition 6.5 implies that $\mathsf{ehr}_P(t)$ is a polynomial of degree d. □

Definition 6.8 (Ehrhart polynomial, h^*-polynomial)**.**
Let $P \subset \mathbb{R}^d$ be d-dimensional lattice polytope.

a) The Ehrhart polynomial $\mathsf{ehr}_P : \mathbb{R} \to \mathbb{R}$ of P is the unique polynomial that extends the Ehrhart counting function $\mathsf{ehr}_P : \mathbb{N}_0 \to \mathbb{R}$.
b) The h^*-polynomial of P is the polynomial $h^* : \mathbb{R} \to \mathbb{R}$ that appears in the numerator of the rational generating function of the Ehrhart series.

Remark 6.9.
If not stated otherwise, we make use of the following notation. The h^*-polynomial of $P \subset \mathbb{R}^d$ is $h^*(t) = \sum_{k=0}^d h_k^* t^k$ and the Ehrhart polynomial of P is $\mathsf{ehr}_P(t) = \sum_{k=0}^d h_k^* \cdot \binom{t+d-k}{d} = \sum_{k=0}^d c_k t^k$.

Corollary 6.10 (Stanley's Monotonicity Theorem)**.**
Let $P, Q \subset \mathbb{R}^d$ be lattice polytopes such that $P \subseteq Q$ and $\dim(Q) = d$. Then $h_k^*(P) \leq h_k^*(Q)$ for the coefficients of the respective h^*-polynomials $h^*(P)$ and $h^*(Q)$.

Proof. If $P \subseteq Q$ then $C(\mathsf{ver}(\widetilde{P})) \subset C(\mathsf{ver}(\widetilde{Q}))$. This immediately implies the claim. □

Corollary 6.11.
If $P \subset \mathbb{R}^d$ is a d-dimensional lattice polytope then the leading coefficient c_d of the Ehrhart polynomial equals the volume $\mathsf{vol}_{\mathbb{R}^d}(P)$ of P, that is, $c_d = \mathsf{vol}_{\mathbb{R}^d}(P)$.

Proof. The d-dimensional volume of the polytope P can be approximated by Riemann sums:

$$\mathsf{vol}_{\mathbb{R}^d}(P) = \int_P 1dx = \lim_{k\to\infty} \frac{1}{k^d}\left|P \cap \frac{1}{k}\mathbb{Z}^d\right| = \lim_{k\to\infty} \frac{1}{k^d}\left|kP \cap \mathbb{Z}^d\right| = \lim_{k\to\infty} \frac{\mathsf{ehr}_P(k)}{k^d} = c_d.$$

□

Definition 6.12 (normalized volume)**.**
The normalized volume of a d-dimensional lattice polytope P is $\mathsf{VOL}_{\mathbb{R}^d}(P) := d! \cdot \mathsf{vol}_{\mathbb{R}^d}(P)$.

Corollary 6.13.
If P is a d-dimensional lattice polytope then $h^*(1) = \sum_{k=0}^d h_k^* = \mathsf{VOL}_{\mathbb{R}^d}(P)$.

Proof. The claim follows immediately from the fact that $\binom{t+d-k}{d}$ has degree d and its leading coefficient is $\frac{1}{d!}$ for all $0 \le k \le d$. □

Corollary 6.14.
If P is a d-dimensional lattice polytope then $c_0 = 1$

Proof. Compute $\mathsf{ehr}_P(0) = \sum_{k=0}^d h_k^* \cdot \binom{0+d-k}{d} = h_0^* \cdot \binom{d}{d}$. Now $\mathsf{ehr}_P(0) = c_0 = 1$ by Stanley's Non-negativity Theorem (Corollary 6.7). □

Corollary 6.15.
If P is a d-dimensional lattice polytope then $h_1^* = \mathsf{ehr}_P(1) - d - 1 = |P \cap \mathbb{Z}^d| - d - 1$.

Proof. Compute $\mathsf{ehr}_P(1) = \sum_{k=0}^d h_k^* \cdot \binom{1+d-k}{d} = h_0^* \cdot \binom{1+d}{d} + h_1^* \cdot \binom{d}{d} = d + 1 + h_1^*$. □

Corollary 6.16.
If P is a d-dimensional lattice polytope then $d!c_k \in \mathbb{Z}$ for all $k \in [d]$.

Proof. Exercise. □

Remark 6.17.
The coefficients $c_1, \dots c_{d-2}$ can be negative. An example with some negative c_k is provided by 'Reeve's simplex' which is defined as $\mathsf{conv}\{0, e_1, e_2, e_1 + e_2 + 18e_3\}$.

6.2. **Lattice in the interior: reciprocity results.**
We first re-examine the three examples of Example 5.2 and verify for these examples the surprising relation $\mathsf{ehr}_{\mathrm{int}(P)}(k) = (-1)^d \cdot \mathsf{ehr}_P(k)$.

Example 6.18.
a) The open line segment $(a, b) \subset \mathbb{R}$ for $a \le b \in \mathbb{Z}$.
We have $\mathsf{ehr}_{(a,b)}k = (k(b-a)+1) - 2 = k(b-a) - 1$ and observe that

$$-\mathsf{ehr}_{(a,b)}k = -\left(k(b-a)-1\right) = (-k)\,(b-a) + 1 = \mathsf{ehr}_{[a,b]}-k.$$

This shows that – up to sign – we compute the number of lattice points in the interior of $k[a, b]$ if we evaluate the Ehrhart polynomial of $[a, b]$ at $-k$.

b) The interior of the standard simplex Δ_d.
If we set $\mathbb{1} := \sum_{i\in[d]} e_i$ then

$$\mathrm{int}(k\Delta_d) \cap \mathbb{Z}^d = \left\{x \in \mathbb{Z}^d \;\middle|\; \begin{smallmatrix} x_i \ge 1 \text{ for all } i \in [d] \\ \text{and } \sum_{i\in[d]} x_i \le k-1 \end{smallmatrix}\right\} = \left\{x \in \mathbb{Z}^d \;\middle|\; \begin{smallmatrix} x_i \ge 0 \text{ for all } i \in [d] \\ \text{and } \sum_{i\in[d]} x_i \le k-1-d \end{smallmatrix}\right\} + \mathbb{1}$$

implies

$$\mathsf{ehr}_{\mathrm{int}(\Delta_d)}(k) = \mathsf{ehr}_{\Delta_d}(k-1-d) = \tbinom{d+k-1-d}{d} = \tbinom{k-1}{d}.$$

But then

$$\tbinom{k-1}{d} = \tbinom{k+d-1-d}{d} = (-1)^d \tbinom{d-k}{d}$$

implies

$$\mathsf{ehr}_{\mathrm{int}(\Delta_d)}(k) = (-1)^d \cdot \mathsf{ehr}_{\Delta_d}(-k).$$

c) The interior of the cube C_d.
Since $\operatorname{int}(kC_d)$ is the product of d open intervals $(0,k)$ and $|(0,k)| \cap \mathbb{Z} = k-1$, we immediately conclude $\mathsf{ehr}_{\operatorname{int}(C_d)}(k) = (k-1)^d$. Notice that

$$\mathsf{ehr}_{\operatorname{int}(C_d)}(k) = (k-1)^d = (-1)^d \cdot (1-k)^d = (-1)^d\left((-k)+1\right) = (-1)^d \mathsf{ehr}_{C_d}(-k).$$

If $\boldsymbol{x} = (x_1, \ldots, x_d) \in (\mathbb{R} \setminus \{0\})^d$ then $\boldsymbol{x}^{-1} := (x_1^{-1}, \ldots, x_d^{-1})$.

Lemma 6.19.
Let $\Lambda \subset \mathbb{R}^d$ be a lattice and $V := \{v_1, \ldots, v_d\} \subset \Lambda$ be primitive vectors. Consider the simplicial cone $C := \mathsf{cone}(V)$ and choose $x_0 \in C$ generic with respect to C. Then

$$\begin{aligned} \rho : \mathsf{Epi}_V(x_0] &\longrightarrow \mathsf{Epi}_V[x_0) \\ x &\longmapsto \sum_{i \in [d]} v_i - x \end{aligned}$$

is a bijection.

Proof. We have

$$\textstyle\sum_{i\in[d]} v_i - y = \sum_{i \in I_+(x_0)} (1-\lambda_i) v_i + \sum_{i \in I_-(x_0)} (1-\mu_i) v_i \in \mathsf{Epi}_V[x_0)$$

for all $y \in \mathsf{Epi}_V(x_0]$. Clearly, the same argument applies to ρ^{-1}. □

Theorem 6.20 (Stanley's Reciprocity Theorem)**.**
Let $\Lambda \subset \mathbb{R}^d$ be a lattice and $V := \{v_1, \ldots, v_d\} \subset \Lambda$ be primitive vectors. Consider the simplicial cone $C := \mathsf{cone}(V)$ together with a triangulation $\mathcal{T}$ of C without new vertices and choose $x_0 \in C$ generic with respect to every $\sigma \in \mathcal{T}_d$. Then

$$\mathsf{G}_C(t) = (-1)^d \cdot \mathsf{G}_{\operatorname{int}(C)}(t^{-1}).$$

Proof. For each $\sigma \in \mathcal{T}_d$ we denote by $V_\sigma \subseteq V$ the set of generators of σ and set $v_\sigma := \sum_{v \in V_\sigma} v$. Then Lemma 6.19 implies

$$\widehat{\mathsf{G}}_{\mathsf{Epi}_{V_\sigma}(x_0]}(t) = \sum_{\boldsymbol{a} \in \mathsf{Epi}_{V_\sigma}(x_0] \cap \mathbb{Z}^d} t^{\boldsymbol{a}} = \sum_{\boldsymbol{a} \in \mathsf{Epi}_{V_\sigma}[x_0) \cap \mathbb{Z}^d} t^{v_\sigma - \boldsymbol{a}} = t^{v_\sigma} \cdot \widehat{\mathsf{G}}_{\mathsf{Epi}_{V_\sigma}[x_0)}(t^{-1}).$$

Therefore

$$\begin{aligned} \mathsf{G}_C(t) &= \sum_{\sigma \in \mathcal{T}_d} \mathsf{G}_{\sigma_{V_\sigma}(x_0]}(t) & &= \sum_{\sigma \in \mathcal{T}_d} \frac{\mathsf{G}_{\mathsf{Epi}_{V_\sigma}[x_0)}(t)}{\prod_{v \in V_\sigma}(1-t^v)} \\ &= \sum_{\sigma \in \mathcal{T}_d} \frac{t^{v_\sigma} \cdot \mathsf{G}_{\mathsf{Epi}_{V_\sigma}(x_0]}(t^{-1})}{\prod_{v \in V_\sigma}(1-t^v)} & &= (-1)^d \sum_{\sigma \in \mathcal{T}_d} \frac{\mathsf{G}_{\mathsf{Epi}_{V_\sigma}(x_0]}(t^{-1})}{t^{-v_\sigma} \cdot \prod_{v \in V_\sigma}(t^v - 1)} \\ &= (-1)^d \sum_{\sigma \in \mathcal{T}_d} \frac{\mathsf{G}_{\mathsf{Epi}_{V_\sigma}(x_0]}(t^{-1})}{\prod_{v \in V_\sigma}(1-t^{-v})} & &= (-1)^d \sum_{\sigma \in \mathcal{T}_d} \mathsf{G}_{\sigma_\sigma[x_0)}(t^{-1}) \\ &= (-1)^d \mathsf{G}_{\operatorname{int}(C)}(t^{-1}) \end{aligned}$$

□

Lemma 6.21.
For $f \in \mathbb{R}[t]$ we set $g^+(t) := \sum_{k \in \mathbb{N}_0} f(k) t^k$ and $g^-(t) := \sum_{k \in \mathbb{N}} f(-k) t^{-k}$. Then $g^+(t) + g^-(t) \equiv 0$.

Proof. It suffices to check the claim for the basis $\left\{ f_k(t) := \binom{t+k}{k} \right\}_{k \in \mathbb{N}_0}$ of $\mathbb{R}[t]$. Then

$$\textstyle\sum_{k \in \mathbb{N}_0} f_m(k) t^k = \sum_{k \in \mathbb{N}_0} \binom{k+m}{m} \cdot t^k = \frac{1}{(1+t)^{m_1}}$$

and

$$\begin{aligned}
\sum_{k\in\mathbb{N}} f_m(-k)t^{-k} &= \sum_{k\in\mathbb{N}} \binom{m-k}{m}\cdot t^{-k} && = \sum_{k\in\mathbb{N}} (-1)^d \binom{k-1}{m}\cdot t^{-k} \\
&= \sum_{k=m+1}^{\infty} (-1)^m \binom{k-1}{m}\cdot t^{-k} && = \sum k\in\mathbb{N}_0 (-1)^m \binom{k+m}{m}\cdot t^{-k-m-1} \\
&= (-1)^m t^{-m-1} \sum_{k\in\mathbb{N}_0} \binom{k+m}{m}\cdot t^{-k} && = (-1)^m t^{-m-1} \frac{1}{(1-t^{-1})^{m+1}} \\
&= \frac{(-1)^m}{t^{m+1}(1-t^{-1})^{m+1}} && = \frac{(-1)^m}{(t-1)^{m+1}} \\
&= -\frac{1}{(1-t)^{m+1}}
\end{aligned}$$

□

Theorem 6.22 (Ehrhart-Macdonald-Reciprocity)**.**
Let $P\subset\mathbb{R}^d$ be a d-dimensional lattice polytope with Ehrhart polynomial $\mathsf{ehr}_P(t)\in\mathbb{R}[t]$. Then

$$\mathsf{ehr}_P(-k) = (-1)^d\cdot\left|\mathrm{int}(kP)\cap\mathbb{Z}^d\right| \qquad \text{for all } k\in\mathbb{N}.$$

Proof. Using Theorem 6.20 (Stanley's Reciprocity Theorem) and Lemma 6.21, we obtain

$$\begin{aligned}
\sum_{k\in\mathbb{N}} \mathsf{ehr}_{\mathrm{int}(P)}(k)\cdot t^k &= \widehat{\mathsf{Ehr}}_{\mathrm{int}(P)}(t) && = \widehat{G}_{\mathrm{int}(C(P))}(1,\ldots,1,t) \\
&= (-1)^{d+1}\widehat{G}_{C(P)}(1,\ldots,1,t^{-1}) && = (-1)^{d+1}\widehat{\mathsf{Ehr}}_P(t^{-1}) \\
&= (-1)^{d+1}\sum_{k\in\mathbb{N}_0} \mathsf{ehr}_P(k)\cdot(t^{-1})^k && = (-1)^d\sum_{k\in\mathbb{N}} \mathsf{ehr}_P(-k)\cdot(t^{-1})^{-k} \\
&= (-1)^d\sum_{k\in\mathbb{N}} \mathsf{ehr}_P(-k)\cdot t^k.
\end{aligned}$$

Now compare coefficients to finish the proof. □

Definition 6.23 (degree and codegree of a polytope)**.**
Let $P\subset\mathbb{R}^d$ be d-dimensional lattice polytope and $h^*(t)$ its h^*-polynomial.
a) The degree $\deg(P)$ of P is defined via $\deg(P) := \max\{k\in\mathbb{N} \mid h_k^*\neq 0\}$.
b) The codegree $\mathrm{codeg}(P)$ of P is defined as $\mathrm{codeg}(P) := d+1-\deg(P)$.

Lemma 6.24.
Let $f\in\mathbb{R}[t]$ be a polynomial of degree $\deg(f)=d$ such that

$$\textstyle\sum_{t\in\mathbb{N}_0} f(t)z^t = \frac{h_0^*+\ldots+h_d^*z^d}{(1-z)^{d+1}}.$$

Then the following statements are equivalent:
a) $h_{k+1}^* = h_{k+2}^* = \ldots = h_d^* = 0$ and $h_k^*\neq 0$.
b) $f(-1) = f(-2) = \ldots = f(-(d-k)) = 0$ and $f(-(d-k+1))\neq 0$.

Proof. Exercise. □

Corollary 6.25.
If $P\subset\mathbb{R}^d$ is a d-dimensional lattice polytope then

$$k_0 = \min\left\{k\in\mathbb{N} \;\middle|\; \mathrm{int}(kP)\cap\mathbb{Z}^d\neq\varnothing\right\} \qquad\Longrightarrow\qquad k_0 = \mathrm{codeg}(P).$$

Proof. The Corollary is a direct consequence of Lemma 6.24 and the Ehrhart-Macdonald-Reciprocity (Theorem 6.22). □

Corollary 6.26.
Let $P \subset \mathbb{R}^d$ be a d-dimensional lattice polytope and $h^*(t)$ its h^*-polynomial. Then the leading coefficient $h^*_{\deg(P)}$ of $h^*(t)$ equals the number of lattice points contained in $\operatorname{int}(P)$*, that is,* $h^*_{\deg(P)} = \left|\operatorname{int}(P) \cap \mathbb{Z}^d\right|$

Proof. Exercise. □

We now classify all possible Ehrhart polynomials lattice polygons in $\mathbb{R}^2$.

Theorem 6.27.
A polynomial $h^*(t) = h^*_2 \cdot t^2 + h^*_1 \cdot t + h^*_0$ with $h^*_0, h^*_1, h^*_2 \in \mathbb{N}$ is the h^*-polynomial of an integer polygon $P \subset \mathbb{R}^2$ if and only if $h^*_0 = 1$ and one of the following statements is true:
a) $h^*_2 = 0$, $h^*_1 \in \mathbb{N}_0$ (then P has no interior points).
b) $h^*_2 = 1$, $h^*_1 = 7$ (then $P \cong 3\Delta_2$).
c) $1 \leq h^*_2 \leq h^*_1 \leq 3h^*_2 + 3$ (then $P \ncong 3\Delta_2$ has interior lattice points).

Proof. For every lattice polygon P with h^*-polynomial $h^*(t) = h^*_2 \cdot t^2 + h^*_1 \cdot t + h^*_0$, we have $h^*_0 = 1$ and $h^*_1, h^*_2 \in \mathbb{N}_0$ by Stanley's Non-negativity Theorem (Corollary 6.7). If we set $i := |\operatorname{int}(P) \cap \mathbb{Z}^2|$ and $b := |\partial P \cap \mathbb{Z}^2|$ then $h^*_1 = b + i - 3$ by Corollary 6.15 and $h^*_2 = i$ by Corollary 6.26.

$\Rightarrow$: If P has no interior points then $h^*_2 = i = 0$ and $h^*_1 = b - 3$. As P has at least three vertices, we conclude *a*). If $P \cong 3\Delta_2$ one directly checks that $h^*_2 = i = 1$ and $h^*_1 = 10 - 3 = 7$. This proves *b*). If $P \ncong 3\Delta_2$ has at least one interior point then we have $h^*_2 = i \geq 1$ as well as $h^*_1 = b + i - 3 \geq h^*_2$ and, combining $\frac{1}{2}\mathsf{vol}_{\mathbb{R}^2}(P) = \frac{1}{2}(1 + h^*_1 + h^*_2)$ with Scott's Theorem (Theorem 1.9), $h^*_1 \leq 3h^*_2 + 3$. This shows *c*).

$\Leftarrow$: We need lattice polygons for each of the three cases. In situation *a*) it is easy to check that $P = \mathsf{conv}\{0, e_1, ke_2\}$ has no interior point and $k + 2$ points on its boundary. Clearly, we have $h^*(t) = t^2 + 7t + 1$ if $P = 3\Delta_2$. Finally, it is easy to check that

$$P := \mathsf{conv}\left\{\binom{0}{0}, \binom{2}{0}, \binom{2}{b-4}, \binom{1}{i+1}\right\}$$

where $b \in \mathbb{N}$ with $b > 4$ and $i \in \mathbb{N}$ with $i \geq \frac{b-6}{2}$ contains precisely i lattice points in its interior and b lattice points on its boundary. This provides an example in situation *c*). □

Remark 6.28.
If we visualize (h_1, h_2) for all possible h^*-polynomials of lattice polygons in $\mathbb{R}^2$ we have either a lattice point on the non-negative h^*_1-axis (situation *a*) or $(7, 1)$ (situation *b*) or a lattice point contained in the (unbounded) polyhedron defined by $h^*_1 \geq 0$, $h^*_2 \geq \frac{1}{3}h^*_1 - 1$ and $h^*_2 \leq h^*_1$.

Corollary 6.29.
The polynomial $c_2t^2 + c_1t + c_0$ is the Ehrhart polynomial $\mathsf{ehr}_P(t)$ of a lattice polygon P if and only if $c_0 = 1$, $2c_1, 2c_2 \in \mathbb{Z}$ with $2c_1 \geq 3$ and one of the following statements is true:
a) $c_1 - c_2 = 1$ (then P has no interior points)
b) $c_1 = c_2 = \frac{9}{2}$ (then $P \cong 3\Delta_2$)
c) $c_1 \leq \frac{1}{2}c_2 + 2$ (then P has at least one interior lattice point)

6.3. **Brion's Theorem.**

In this section, we show that the integer point generating function of a d-dimensional lattice polytope $P \subset \mathbb{R}^d$ can be expressed in terms of integer point generating functions of (affine) cones associated to vertices of P. We first introduce the notion of a tangent cone T_vP associated to a face F in P.

Definition 6.30 (tangent cone)**.**
Let $P \subset \mathbb{R}^d$ be a d-polytope and F a face of P. The tangent cone T_FP of F in P is defined as

$$T_FP := \left\{x \in \mathbb{R}^d \;\middle|\; \begin{smallmatrix}(1-\varepsilon)p+\varepsilon x \in P \\ \text{for all } p \in F \text{ and } 0 < \varepsilon \leq 1\end{smallmatrix}\right\}.$$

Remark 6.31.

i) The viligant reader may notice that the tangent cone is not a polyhedral cone as defined in Definition 3.1. The tangent cone is rather an affine polyhedral cone, that is, $(-x)+T_FP$ is a polyhedral cone for any $x \in F$ (as defined in Definition 3.1).
ii) For polytope aficionados only: the polyhedral cone that is dual to $(-x)+T_FP$ coincides with the normal cone of F in P.
iii) An alternative description of T_FP can be given in terms of halfspaces that define P. Let P be given as intersection of halfspaces $H_1^{\geq}, \ldots, H_n^{\geq}$ with bounding hyperplanes $H_1, \ldots, H_n$. Then

$$T_FP = \bigcap_{H_i \supset F} H_i^{\geq}.$$

Theorem 6.32 (Brianchon-Gram)**.**
Let $P \subset \mathbb{R}^d$ be a lattice d-polytope. Then

$$\widehat{\mathsf{G}}_P(\boldsymbol{t}) = \sum_{\varnothing \neq F \preccurlyeq P} (-1)^{\dim(F)}\, \widehat{\mathsf{G}}_{T_FP}(\boldsymbol{t}).$$

Proof. We write $\widehat{\mathsf{G}}_P(\boldsymbol{t}) = \sum_{\boldsymbol{a} \in \mathbb{Z}^d} \lambda_{\boldsymbol{a}}\, \boldsymbol{t}^{\boldsymbol{a}}$ where almost all $\lambda_{\boldsymbol{a}} = 0$ and compare coefficients for each monomial $\boldsymbol{t}^{\boldsymbol{a}}$. Let $f(P) = (f_0(P), \ldots, f_d(P)) \in \mathbb{Z}^{d+1}$ be the f-vector of P, that is, $f_i(P)$ counts the i-dimensional faces of P. We now distinguish the two possible cases $\boldsymbol{a} \in P$ and $\boldsymbol{a} \notin P$.

Case 1 ($\boldsymbol{a} \in P$):
If $\boldsymbol{a} \in P$ then $\boldsymbol{a} \in T_FP$ for every face F of P and we conclude that the coefficient of $\boldsymbol{t}^{\boldsymbol{d}}$ on the right-hand side equals

$$\sum_{\varnothing \neq F \preccurlyeq P} (-1)^{\dim(F)} = \sum_{i=0}^{d} (-1)^i f_i(P) = 1.$$

The last equality is a consequence of the Euler-Poincaré-formula for polytopes (see exercises for details).

Case 2 ($\boldsymbol{a} \in \mathbb{R}^d \setminus P$):
Let $\mathcal{H}$ be the set of closed half-spaces that define P, that is, $P = \bigcap_{H \in \mathcal{H}} H$. Moreover, let $H^=$ be the (affine) hyperplane that bounds $H \in \mathcal{H}$ and $\mathcal{H}^F := \{H \in \mathcal{H} \mid F \subset H^=\}$ for every proper face $F \prec P$. Now set

$$S_{\boldsymbol{a}} := \left\{ F \prec P \;\middle|\; \boldsymbol{a} \notin H \text{ for each } H \in \mathcal{H}^F \right\}.$$

Then $\boldsymbol{a} \in T_FP$ if and only if $F \notin S_{\boldsymbol{a}}$. We additionally consider the closure of $S_{\boldsymbol{a}}$ and define

$$K := \{G \prec P \mid G \preccurlyeq F \text{ for some } F \in S_{\boldsymbol{a}}\}.$$

Clearly, K is a polyhedral complex of dimension $\dim(F)$ and we extend its f-vector $f(K) = (f_0(K), \ldots, f_d(K)) \in \mathbb{Z}^d$ by $f_i(K) = 0$ for $i > \dim(F)$. Then the coefficient of the right-hand side equals

$$\sum_{i=0}^{d} (-1)^i \left(f_i(P) - f_i(K)\right) = 1 - \sum_{i=0}^{\dim(F)} (-1)^i f_i(K) = 1 - 1 = 0.$$

□

Before we state Brion's Theorem, we consider the following 1-dimensional example which motivates to extend the homomorphism Φ beyond summable Laurent series.

Example 6.33.
If $P := [0;3]$ then $\widehat{\mathsf{G}}_P(t) = t^0 + t^1 + t^3 = \mathsf{G}_P(t)$. The two 1-dimensional cones

$$C^+ := [0;\infty] \qquad \text{and} \qquad C^- := [-\infty, 3]$$

satisfy $P = C^+ \cap C^-$ as well as

$$\widehat{\mathsf{G}}_{C^+}(t) = \sum_{k \in \mathbb{N}_0} t^k, \qquad \text{and} \qquad \widehat{\mathsf{G}}_{C^-}(t) = \sum_{k \in \mathbb{N}_0} t^{3-k} = t^3 \cdot \sum_{k \in \mathbb{N}_0} \left(\tfrac{1}{t}\right)^k.$$

As $\widehat{\mathsf{G}}_{C^+}(t)$ is a summable Laurent series in t and $\widehat{\mathsf{G}}_{C^-}(t)$ is a summable Laurent series in $\tilde{t} = \frac{1}{t}$, we compute

$$\mathsf{G}_{C^+}(t) = \Phi\left(\widehat{\mathsf{G}}_{C^+}(t)\right) = \frac{1}{1-t} \qquad \text{and} \qquad \mathsf{G}_{C^-}(t) = \Phi\left(\widehat{\mathsf{G}}_{C^-}\left(\tilde{t}\right)\right) = \tilde{t}^{-3} \cdot \frac{1}{1-\tilde{t}} = -\frac{t^4}{1-t}.$$

As a consequence, we obtain the somehow surprising identity

$$\mathsf{G}_P(t) = t^0 + t^1 + t^3 = \frac{1}{1-t} - \frac{t^4}{1-t} = \mathsf{G}_{C^+}(t) + \mathsf{G}_{C^-}(t).$$

that can be summarized on a more abstract level using the linearity of Φ:

$$\mathsf{G}_P(t) = \frac{1}{1-t} - \frac{t^4}{1-t} = \Phi\left(\widehat{\mathsf{G}}_{C^+}(t)\right) + \Phi\left(\widehat{\mathsf{G}}_{C^+}(t)\right) = \Phi\left(\widehat{\mathsf{G}}_{C^+}(t) + \widehat{\mathsf{G}}_{C^+}(t)\right).$$

Now $\widehat{\mathsf{G}}_{C^+}(t) + \widehat{\mathsf{G}}_{C^-}(t)$ counts points of $\mathbb{R} \setminus P$ once and points of P twice and we conclude

$$\mathsf{G}_P(t) = \Phi\left(\widehat{\mathsf{G}}_{\mathbb{R}}(t) + \widehat{\mathsf{G}}_P(t)\right).$$

In particular, the linearity of Φ suggests $\Phi\left(\widehat{\mathsf{G}}_{\mathbb{R}}(t)\right) = 0$. However, we emphasize that $\Phi\left(\widehat{\mathsf{G}}_{\mathbb{R}}(t)\right)$ is not defined yet as $\widehat{\mathsf{G}}_{\mathbb{R}}(t)$ is not a summable Laurent series.

Proposition 6.34.
Let $\varphi : \widehat{\mathsf{L}}^{sum} \to \mathbb{R}(t_1, \ldots, t_d)$ be a homomorphism of L-modules and $\widetilde{\varphi} : \mathsf{L} \to \mathbb{R}(t_1, \ldots, t_d)$ be a homomorphism extending φ to the integer point series of polyhedral cones C with $\operatorname{lineal}(C) \neq \{0\}$. *Then*

$$\widetilde{\varphi}\left(\widehat{\mathsf{G}}_C(\boldsymbol{t})\right) = 0 \qquad \textit{for all polyhedral cones } C \textit{ with } \operatorname{lineal}(C) \neq \{0\}.$$

Proof. If $\boldsymbol{x} = (x_1, \ldots, x_d) \in \operatorname{lineal}(C) \setminus \{0\}$ then $\mathsf{span}_{\mathbb{R}}(\boldsymbol{x}) \subseteq C$ and $\boldsymbol{t}^{\boldsymbol{x}} \cdot \widehat{\mathsf{G}}_C(\boldsymbol{t}) = \widehat{\mathsf{G}}_C(\boldsymbol{t})$. Thus

$$\widetilde{\varphi}\left(\widehat{\mathsf{G}}_C(\boldsymbol{t})\right) = \varphi\left(\boldsymbol{t}^{\boldsymbol{x}} \cdot \widehat{\mathsf{G}}_C(\boldsymbol{t})\right) = \boldsymbol{t}^{\boldsymbol{x}} \cdot \varphi\left(\widehat{\mathsf{G}}_C(\boldsymbol{t})\right)$$

which implies $(1 - \boldsymbol{t}^{\boldsymbol{x}})\widetilde{\varphi}\left(\widehat{\mathsf{G}}_C(\boldsymbol{t})\right) = 0$. Since $(1 - \boldsymbol{t}^{\boldsymbol{x}}) \neq 0$ and $\mathbb{R}(t_1, \ldots, t_d)$ is an integral domain, we conclude that $\widetilde{\varphi}\left(\widehat{\mathsf{G}}_C(\boldsymbol{t})\right) = 0$. □

As a consequence of Proposition 6.34, we extend the homorphism $\Phi : \widehat{\mathsf{L}}^{sum} \to \mathbb{R}(t_1, \ldots, t_d)$ to all integer point series of polyhedral cones with $\operatorname{lineal}(C) \neq \{0\}$ by

$$\widetilde{\Phi}\left(\widehat{\mathsf{G}}_C(\boldsymbol{t})\right) := \begin{cases} \Phi\left(\widehat{\mathsf{G}}_C(\boldsymbol{t})\right), & C \text{ is polyhedral cone with } \operatorname{lineal}(C) = \{0\}, \\ 0, & C \text{ is polyhedral cone with } \operatorname{lineal}(C) \neq \{0\}. \end{cases}$$

As this extension is unique, we abuse notation and denote the extension $\widetilde{\Phi}$ by Φ.

Theorem 6.35 (Brion's Theorem)**.**
Let $P \subset \mathbb{R}^d$ be a lattice d-polytope with vertex set $\mathsf{V}(P)$. Then

$$\mathsf{G}_P(\boldsymbol{t}) = \sum_{v \in \mathsf{V}(P)} \mathsf{G}_{T_v P}(\boldsymbol{t}).$$

Proof. Apply Φ to both sides of the identity of the Theorem by Brianchon-Gram (Theorem 6.32) and notice that the only tangetial cones $T_F P + (-x)$ with $\operatorname{lineal}(T_F P + (-x)) \neq \{0\}$ for $x \in F$ correspond to faces F with $\dim(F) = 0$. □

7. Counting lattice points: algorithmic aspects

7.1. The basic idea of Barvinok's algorithm.

The goal of this section is to present an algorithm to compute the number of lattice points contained in a lattice polytope which is essentially due to Barvinok (1994). The algorithm has been successfully implemented, available software packages are `latte` and `barvinok`. The running time of Barvinok's algorithm is polynomial in the input size if the dimension of the polytope is fixed. A key ingredient in our presentation is an algorithm due to Lenstra, Lenstra and Lovasz (1983) that is fundamental to integer programming although Barvinok's original approach divised a different algorithm. Dyer and Kannan (1997) used the LLL-algorithm for the first time in this context.

The fundamental idea of Barvinok's algorithm is fairly simple: Starting with a d-polytope $P \subset \mathbb{R}^d$ with vertex set $\mathsf{V}(P) \subset \Lambda$ for some lattice Λ, we have

$$\mathsf{G}_P(t) = \sum_{v \in \mathsf{V}(P)} \mathsf{G}_{T_v P}(t)$$

by Brion's Theorem. If P is not simple then there are non-simplicial tangential cones $T_v P$ and we subdivide all tangential cones into simplicial cones $\widetilde{C}_i$ and compute Λ-primitive generators for $\widetilde{C}_i$ that span associated lattices $\widetilde{\Gamma}_i$. We set $\det(\widetilde{C}_i) := |\Lambda/\widetilde{\Gamma}_i|$ and have $\det(\widetilde{C}_i) = 1$ if and only if $\widetilde{\Gamma}_i$ is unimodular. Moreover, if $\widetilde{\Gamma}_i$ is not unimodular and if we want to count lattice points of $\widetilde{C}_i \cap \Lambda$ then we have essentially two choices: either we find the lattice points in $\Pi_{\widetilde{\Gamma}_i}$ or we find a unimodular subdivision. If we manage to find a Λ-primitive vector $v \in \widetilde{C}_i \cap \Lambda$, we can subdivide $\widetilde{C}_i$ into cones D_k that satisfy $\det(D_k) < \det(C_i)$ for all k. Iterating this process yields a decomposition of the tangential cones $T_v P$ into unimodular simplicial cones. Unfortunately, there are two problems related to this approach. First of all, we have to guarantee that we quickly find a vector v to subdivide $\widetilde{C}_i$ into cones D_k. Second, we have pay attention to the number of cones used for unimodular subdivisions. Unfortunately, this number is not universally bounded as the following example for $\mathbb{Z}^2 \subset \mathbb{R}^2$ shows.

Example 7.1.
For $\Lambda = \mathbb{Z}^2 \subset \mathbb{R}^2$ and $k \in \mathbb{N}$, consider the simplicial cone $C_k = \mathsf{cone}\{\binom{1}{0}, \binom{1}{k}\}$. Clearly, the generators are primitive and C_k has a unique unimodular subdivision into k cones

$$C_k^j = \mathsf{cone}\left\{\binom{1}{j-1}, \binom{1}{j}\right\}$$

where $j \in [k]$. In particular, even in dimension 2 there is no upper bound on the number of 2-dimensional cones needed for a unimodular subdivision.

Example 7.1 shows that there is no algorithm that computes the number of lattice points of a polytope in polynomial time and that relies on unimodular *subdivisions*. Barvinok suggests a smarter use of unimodular cones and uses *signed decompositions* of simplicial cones: he allows addition and substraction of cones. It turns out that the number of maximal cones used for such a decomposition of a simplical cone C is of the order $(\ln \det(C))^{O(d^2 \ln d)}$ which allows computations in practice.

Before we explain Barvinok's approach in more detail, we discuss how to find short lattice vectors $w \in \Lambda$, a tool needed for the signed decompositions. Moreover, we state a classical result of Minkowski that implies the existence of w inside a bounded convex centrally symmetric set K if $\mathsf{vol}_{\mathbb{R}^d}(K)$ is sufficiently large. The proof is not difficult but we defer it to Section **??**.

Theorem 7.2 (Minkowski's First Convex Body Theorem, 1894)**.**
Consider a lattice $\Lambda \subset \mathbb{R}^d$ of rank d and let $K \subset \mathbb{R}^d$ be a compact and Lebesgue measurable set that is convex ($\frac{x+y}{2} \in K$ for all $x, y \in K$), centrally symmetric ($-x \in K$ for all $x \in K$) and satisfies $\mathsf{vol}_{\mathbb{R}^d}(K) \geq 2^d \det(\Lambda)$. Then

$$|K \cap \Lambda \setminus \{0\}| \geq 1.$$

We apply this theorem to our situation. Consider a d-dimensional cone $\widetilde{C} = \mathsf{cone}(v_1, \ldots, v_d)$ generated by Λ-primitive vectors and let $\widetilde{\Gamma} = \mathsf{span}_{\mathbb{Z}}\{v_1, \ldots, v_d\}$ be the associated sublattice of Λ with fundamental parallelepiped $\Pi_{\widetilde{\Gamma}}$. Moreover, let

$$K := \left\{ x = \sum_{i\in[d]} \lambda_i v_i \;\middle|\; |\lambda_i| \leq 1 \text{for all } i \in [d] \right\}$$

be a centrally symmetric modification of $\Pi_{\widetilde{\Gamma}}$. Recall that the index of $\widetilde{\Gamma}$ in Λ is

$$|\Lambda/\widetilde{\Gamma}| = |\Pi_{\widetilde{\Gamma}} \cap \Lambda| = \frac{|\det(\widetilde{\Gamma})|}{|\det(\Lambda)|} = \frac{\mathsf{vol}_{\mathbb{R}^d}(\Pi_{\widetilde{\Gamma}})}{\mathsf{vol}_{\mathbb{R}^d}(\Pi_\Lambda)}.$$

If $|\Lambda/\widetilde{\Gamma}| > 1$ then the $\frac{1}{\sqrt[d]{|\Lambda/\widetilde{\Gamma}|}}$-dilate $\widetilde{K}$ of K has volume $2^d \det(\Lambda)$ and Theorem 7.2 guarantees the existence of a nontrivial element $w \in \widetilde{K} \cap \Lambda \setminus \{0\}$ and $0 \leq |\lambda_i| \leq \frac{1}{\sqrt[d]{|\Lambda/\widetilde{\Gamma}|}}$ if $w = \sum_{i\in[d]} \lambda_i v_i$.

Minkowski's Theorem does not provide a construction of a nontrivial lattice point $w \in \widetilde{K}$ and it is not clear how to find w. A celebrated result due to Lenstra, Lenstra and Lovász can be used to find w as we explain next, details and a proof of the Theorem will be given a in Section 7.2.

Theorem 7.3 (Lenstra, Lenstra & Lovász, 1982)**.**
For every $d \in \mathbb{N}$ there exists a universal constant M that depends only on d such that the following statement holds for every lattice Λ of rank d that is given by a lattice basis $\mathcal{B}_\Lambda \subset \mathbb{Z}^d$.

There is a lattice basis $v_1, \ldots, v_d$ for Λ that satisfies $\prod_{i\in[d]} \|v_i\| \leq M \cdot \det(\Lambda)$ and this lattice basis can be constructed from $\mathcal{B}_\Lambda$ in polynomial time in d and the input size of Λ.

A valid choice for M is $2^{\frac{d(d-1)}{4}} = 2^{\frac{1}{2}\binom{d}{2}}$ as we will show in Corollary 7.11. An advantage of the basis constructed in Theorem 7.3 is that all coefficients of a shortest vector $w \in \Lambda \setminus \{0\}$ with respect to this basis are bounded by $M\sqrt{d}$.

Lemma 7.4.
Let $\Lambda \subset \mathbb{R}^d$ be a lattice given by a lattice basis $\mathcal{B}_\Lambda = \{v_1, \ldots, v_d\} \subset \mathbb{Z}^d$. Choose $M \in \mathbb{N}$ such that $\|v_i\| \cdot \ldots \cdot \|v_d\| \leq M \cdot \det(\Lambda)$. If $w \in \Lambda \setminus \{0\}$ is a shortest nontrivial vector of Λ then

$$w = \sum_{i\in[d]} \lambda_i v_i \text{ with } 0 \leq |\lambda_i| \leq M\sqrt{d}.$$

Proof. We have $w = V\lambda$ and $\lambda = V^{-1}w$ where

$$V := \begin{pmatrix} | & & | \\ v_1 & \cdots & v_d \\ | & & | \end{pmatrix} \in \mathbb{R}^{d\times d} \qquad \text{and} \qquad \lambda := \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_d \end{pmatrix}.$$

Cramer's rule implies that the entries of V^{-1} are signed $((d-1)\times(d-1))$-minors of V multiplied by $\frac{1}{\det(V)}$. If we relabel the v_i such that $\|v_1\| \leq \|v_j\|$ for $2 \leq j \leq d$ then the relevant minors are bounded by $\|v_2\| \cdot \ldots \cdot \|v_d\|$ and we obtain

$$|(V^{-1})_{ij}| \leq \frac{\|v_2\| \cdot \ldots \cdot \|v_d\|}{\det(V)} \leq \frac{M}{\|v_1\|}$$

for all $i, j \in [d]$. A standard inequality between the ℓ_1-norm and the euclidean norm as well as $\|w\| \leq \|v_1\|$ imply

$$|\lambda_i| \leq \frac{M}{\|v_1\|} \cdot \sum_{i\in[d]} |w_i| \leq \frac{M}{\|v_1\|} \cdot \sqrt{d}\|w\| \leq M\sqrt{d}.$$

□

Corollary 7.5.
Let $d \in \mathbb{N}$, M be a constant as described in Theorem 7.3 and Λ be a lattice of rank d with lattice basis $\mathcal{B}_\Lambda \subset \mathbb{Z}^d$. Then a nontrivial shortest vector $w \in \Lambda \setminus \{0\}$ can be found in polynomial time in the input size of Λ.

Proof. If Λ is given by the lattice basis $\mathcal{B}_\Lambda = \{\widetilde{v}_1, \ldots, \widetilde{v}_d\}$ then a new basis $v_1, \ldots, v_d$ that satisfies

$$\|v_1\| \cdot \ldots \cdot \|v_d\| \leq M \cdot \det(\Lambda)$$

can be constructed in time that is polynomial in the input size of $\mathcal{B}_\Lambda$ since d is fixed. By Lemma 7.4, we have to enumerate at most $(2\lfloor\sqrt{d}\rfloor M+1)^d$ vectors to identify a nontrivial shortest vector in Λ. This proves the claim. □

To apply Corollary 7.5 to our original problem we need a little twist as we are looking for a shortest vector $w \in \Lambda \setminus \{0\}$ that additionally satisfies $w \in \widetilde{K}$. First, consider the linear transformation $T : \mathbb{R}^d \longrightarrow \mathbb{R}^d$ that maps v_i to the standard basis vector e_i for all basis vectors $v_1, \ldots, v_d$ of $\widetilde{\Gamma}$. Then apply T to a lattice basis $\mathcal{B}_\Lambda$ of Λ to obtain a lattice basis $\mathcal{B}_{T(\Lambda)}$ of $T(\Lambda)$ and follow Corollary 7.5 and search for a shortest vector

$$w_0 \in T(\Lambda) \setminus \{0\} \text{ that additionally satisfies } w_0 \in \left[-\tfrac{1}{\sqrt[d]{|\Lambda/\widetilde{\Gamma}|}}; \tfrac{1}{\sqrt[d]{|\Lambda/\widetilde{\Gamma}|}}\right]^d.$$

Then $w := T^{-1}(w_0) \in \Lambda \setminus \{0\}$ satisfies $w \in \widetilde{K}$. Notice that we may assume As $\widetilde{K}$ is centrally symmetric, we can assume without loss of generality that w and $v_1, \ldots, v_d$ are contained in a common half-space.

Using w, we now construct d new cones from $\widetilde{C} = \mathsf{cone}(v_1, \ldots, v_d)$ and define

$$D_i := \mathsf{cone}(v_1, \ldots, v_{i-1}, w, v_{i+1}, \ldots, v_d)$$

for $i \in [d]$. Of course, we also have d associated sublattices Γ_i of Λ defined as

$$\Gamma_i := \mathsf{span}_{\mathbb{Z}}(v_1, \ldots, v_{i-1}, w, v_{i+1}, \ldots, v_d)$$

with index

$$|\Lambda/\Gamma_i| = \frac{|\det(\Gamma_i)|}{|\det(\Lambda)|} = |\lambda_i| \cdot \frac{|\det(\widetilde{\Gamma})|}{|\det(\Lambda)} = |\lambda_i| \cdot |\Lambda/\widetilde{\Gamma}| \leq |\Lambda/\widetilde{\Gamma}|^{\frac{d-1}{d}} < |\Lambda/\widetilde{\Gamma}|$$

if Γ_i has rank d. In particular, the index $|\Lambda/\Gamma_i|$ is strictly smaller than $|\Lambda/\widetilde{\Gamma}|$ and we can iterate this construction until all cones are unimodular. But can we recover $\widetilde{C}$ from $D_1, \ldots, D_d$? To that respect, define

$$\epsilon_i := \begin{cases} 1 & (v_1, \ldots, v_d) \text{ and } (v_1, \ldots, v_{i-1}, w, v_{i+1}, \ldots, v_d) \text{ have the same orientation;} \\ -1 & (v_1, \ldots, v_d) \text{ and } (v_1, \ldots, v_{i-1}, w, v_{i+1}, \ldots, v_d) \text{ do not have the same orientation;} \\ 0 & v_1, \ldots, v_{i-1}, w, v_{i+1}, \ldots, v_d \text{ are linearly dependent.} \end{cases}$$

The idea is now to consider the signed decomposition $\sum_{i\in[d]} \epsilon_i D_i$ were we first take the union of all simplices with $\epsilon_i = 1$ and then remove the simplices with $\epsilon_i = -1$. More precisely, we have to take multiplicities of points into account that arise from non-empty intersections of cones. A possible way to avoid careful and cumbersome book-keeping due to inclusion-exclusion is the use of half-open cones. This has been proposed by Köppe and Verdoolaege in 2008.

7.2. **A universal tool: the LLL-algorithm.**

In this section we discuss and proof the Lenstra-Lenstra-Lovász-Theorem 7.3. Lemma 7.6 and Lemma 7.7 are technical results that we need to prove the LLL-Theorem. They are direct consequences of Minkowski's First Convex Body Theorem 7.2. After a brief recall on the Gram-Schmidt-orthogonalization, we define weakly reduced lattice bases as well as reduced lattice bases and prove the LLL-Theorem 7.3.

Lemma 7.6.
Let $\Lambda \subset \mathbb{Z}^d \subset \mathbb{R}^d$ be lattice with $\mathsf{rk}(\Lambda) = d$. Then there exists a nontrivial $v \in \Lambda \setminus \{0\}$ such that

$$\|v\| \leq \sqrt{d}\sqrt[d]{\det(\Lambda)}.$$

Proof. The lemma follows directly from Minkowski's First Convex Body Theorem.

□

Now consider a basis $\mathcal{B} = \{v_1, \dots, v_d\}$ of $\Lambda \subset \mathbb{R}^d$ and a compatible flag of subspaces defined as

$$V_0 := \{0\} \qquad \text{and} \qquad V_k := \mathsf{span}_{\mathbb{R}}(v_1, \dots, v_k) \text{ for } k \in [d].$$

Moreover, we set

$$\Lambda_k := \Lambda \cap V_k \qquad \text{and} \qquad D(v_1, \dots, v_d) := \prod_{k \in [d-1]} \det(\Lambda_k).$$

Lemma 7.7.
If $\lambda_1 = \min\{\|u\| \mid u \in \Lambda \setminus \{0\}\}$ *then*

$$\lambda_1^{\frac{d(d-1)}{2}} \prod_{k \in [d-1]} k^{-\frac{k}{2}} \leq D(v_1, \dots, v_d).$$

Proof. As $\lambda_1 \leq \min\{\|u\| \mid u \in \Lambda_k \setminus \{0\}\}$ for all $k \in [d]$, Lemma 7.6 implies

$$\lambda_1 \leq \min\{\|u\| \mid u \in \Lambda_k \setminus \{0\}\} \leq \sqrt{k}\sqrt[k]{\det(\Lambda_k)}.$$

This implies $\left(\frac{\lambda_1}{\sqrt{k}}\right)^k \leq \det(\Lambda_k)$ and thus

$$D(v_1, \dots, v_d) = \prod_{k \in [d-1]} \det(\Lambda_k) \geq \prod_{k \in [d-1]} \left(\frac{\lambda_1}{\sqrt{k}}\right)^k = \lambda_1^{\frac{d(d-1)}{2}} \prod_{k \in [d-1]} k^{-\frac{k}{2}}.$$

□

The basic tool for the Lenstra-Lenstra-Lovász-Theorem is the Gram-Schmidt-orthogonalization (not ortho*normalization*!). Recall that the projection

$$\pi_k : \mathbb{R}^d \longrightarrow V_k \qquad \text{defined via} \qquad x \longmapsto \sum_{i \in [k]} \frac{\langle x, v_i \rangle}{\langle v_i, v_i \rangle} v_i$$

yields pairwise orthogonal vectors $w_k := v_k - \pi_{k-1}(v_k)$ for $k \in [d]$ that satisfy

$$\det(\Lambda_k) = \prod_{i \in [k]} \|w_i\|$$

for all $k \in [d]$. Moreover, there exist $\lambda_{ij} \in \mathbb{R}$ for $1 \leq j < i \leq d$ such that

$$v_i = w_i + \sum_{j \in [i-1]} \lambda_{ij} w_j \tag{1}$$

for all $i \in [d]$.

Definition 7.8 (weakly reduced basis, reduced basis)**.**
Let $\mathcal{B} = \{v_1, \dots, v_d\}$ be a lattice basis of a lattice $\Lambda \subset \mathbb{R}^d$ and $\widetilde{\mathcal{B}} = \{w_1, \dots, w_d\}$ the Gram-Schmidt-orthogonalization of $\mathcal{B}$.

i) Then $\mathcal{B}$ is a *weakly reduced basis* of Λ if

$$|\lambda_{ij}| \leq \frac{1}{2}$$

for all $1 \leq j < i \leq d$ where the λ_{ij} are implicitly defined by (1) .

ii) $\mathcal{B}$ is a *reduced basis* of Λ if $\mathcal{B}$ is a weakly reduced basis of Λ and

$$\mathsf{dist}(v_k, V_{k-1}) \leq \sqrt{\frac{4}{3}} \cdot \mathsf{dist}(v_{k+1}, V_{k-1})$$

for all $k \in [d-1]$.

The geometric meaning of a reduced basis is obvious: the distance of v_{k+1} to the subspace V_{k-1} is not much closer than the disctance of v_k to V_{k-1} for all $k \in [d-1]$.

The LLL-algorithm to construct a basis as claimed in Theorem 7.3 consists of two steps:

i) Construct a weakly reduced basis $\widetilde{\mathcal{B}}$ from a lattice basis $\mathcal{B}$.

ii) Transform the weakly reduced lattice basis $\widetilde{\mathcal{B}}$ constructed in Step i) into a reduced basis.

Step 1 of LLL-algorithm: Construct a weakly reduced basis from a lattice basis of Λ.
Recall Equation (1) for all $i \in [d]$:

$$v_i = w_i + \sum_{j\in[i-1]} \lambda_{ij} w_j.$$

If $|\lambda_{k\ell}| > \frac{1}{2}$ for some $1 \leq \ell < k \leq d$ then there exist unique $\mu_{k\ell} \in \mathbb{R}$ and $a_{k\ell} \in \mathbb{Z}$ such that

$$|\mu_{k\ell}| \leq \frac{1}{2} \qquad \text{and} \qquad \lambda_{k\ell} = \mu_{k\ell} + a_{k\ell}.$$

If we replace v_k by $\widetilde{v}_k := v_k - a_{k\ell} v_\ell$ then the subspaces V_j remain invariant for all $0 \leq j \leq d$ since $\ell < k$. Similarly, the Gram-Schmidt-orthogonalization $\widetilde{\mathcal{B}} = \{w_1, \ldots, w_d\}$ is unchanged and $\{v_1, \ldots, v_j\}$ (where the new $\widetilde{v}_k$ replaces the old v_k) remains a lattice basis of Λ_j for all $j \in [d]$. We inspect Equations (1) once more and observe that the only coefficients λ_{ij} that might change are those involved in the representation of v_k. More precisely, we have

$$\widetilde{v}_k = v_k - a_{k\ell} v_\ell = w_k + \sum_{j\in[k-1]} \lambda_{kj} w_j - a_{k\ell} v_\ell = w_k + \sum_{j\in[\ell]} (\lambda_{kj} - a_{k\ell}\eta_j) w_j + \sum_{j=\ell+1}^{k-1} \lambda_{kj} w_j$$

where $v_\ell = \sum_{j\in[\ell]} \eta_j w_j$ as $v_\ell \in V_\ell$. Notice that $\eta_\ell = 1$ which implies $|\lambda_{k\ell} - a_{k\ell}\eta_\ell| = |\mu_{k\ell}| \leq \frac{1}{2}$. Thus, the coefficient $\lambda_{k\ell}$ for the new basis vector $\widetilde{v}_k$ satisfies the condition for a weakly reduced basis and to achieve this, we only changed λ_{kj} for $j < k$. So, we can construct a weakly reduced basis if we modify $\lambda_{k\ell}$ for the largest ℓ and and iterate to modify $\lambda_{k\ell'}$ for $\ell' < \ell$ if necessary. There are at most $\binom{d}{2}$ coefficents $\lambda_{k\ell}$ that we have to modify and while modifying $\lambda_{k\ell}$ we adjust at most $\ell \leq d$ other coefficients λ_{kj}, we conclude that we construct a weakly reduced basis in $O(d^3)$ steps.

Step 2 of LLL-algorithm: Transform a weakly reduced basis into a reduced basis of Λ.
We use Step 1 of the LLL-algorithm as an intermediate step. Let $\mathcal{B}$ be a weakly reduced basis provided by Step 1. If $\mathcal{B}$ is a reduced basis then output $\mathcal{B}$. If $\mathcal{B} = \{v_1, \ldots, v_d\}$ (with associated flag of subspaces $V_0, \ldots, V_d$ and Gram-Schmidt basis $\{w_1, \ldots, w_d\}$) is not a reduced basis then

$$\mathsf{dist}(v_k, V_{k-1}) > \sqrt{\frac{4}{3}} \cdot \mathsf{dist}(v_{k+1}, V_{k-1}) \tag{2}$$

for some $k \in [d-1]$. If we swap v_k and v_{k+1} to obtain $\overline{\mathcal{B}} := \{\bar{v}_1, \ldots, \bar{v}_d\}$ then

$$\mathsf{dist}(\bar{v}_k, V_{k-1}) \leq \sqrt{\frac{4}{3}} \cdot \mathsf{dist}(\bar{v}_{k+1}, V_{k-1}).$$

We output $\overline{\mathcal{B}}$ if it is a reduced basis and otherwise we apply Step 1 (if necessary) to $\overline{\mathcal{B}}$ to obtain a new weakly reduced basis $\mathcal{B} = \{v_1, \ldots, v_d\}$ that satisfies $\mathsf{dist}(v_k, V_{k-1}) \leq \sqrt{\frac{4}{3}} \cdot \mathsf{dist}(v_{k+1}, V_{k-1})$.

Iterating Step 2 outputs a reduced basis unless we cycle endlessly. To prove that Step 2 does terminate after finitely many steps, we use the lower bound for $D(v_1, \ldots, v_d)$ provided by Lemma 7.7 and show that each iteration of Step 2 strictly decreases $D(v_1, \ldots, v_d)$.

To compare the value of D before and after each iteration, we first notice that an application of Step 1 to a lattice basis does not change $D(v_1, \ldots, v_d)$: the lattices Λ_k remain unchanged because the flag of subspaces $V_0, \ldots, V_d$ is invariant. Therefore it suffices to analyze how $D(v_1, \ldots, v_d)$ is affected by a swap that changes $\mathcal{B}$ into $\overline{\mathcal{B}}$. We denote the Gram-Schmidt basis associated to $\overline{\mathcal{B}}$ by $\{\overline{w}_1, \ldots, \overline{w}_d\}$, the flag of subspaces by $\overline{V}_0, \ldots, \overline{V}_d$ and the lattices by $\overline{\Lambda}_0, \ldots, \overline{\Lambda}_d$. Then

$$\overline{V}_i = V_i \text{ for } i \in [d] \setminus \{k\} \qquad \text{and} \qquad \overline{V}_k = \mathsf{span}_{\mathbb{R}}(v_1, \ldots, v_{k-1}, v_{k+1}).$$

as well as $\overline{w}_i = w_i$ for all $i \in [d] \setminus \{k\}$ and Equation (2) implies $\|\overline{w}_k\| < \sqrt{\frac{3}{4}} \|w_k\|$. This implies

$$\det(\overline{\Lambda}_k) < \frac{\sqrt{3}}{2} \cdot \det(\Lambda_k) \qquad \text{and} \qquad D(\overline{v}_1, \ldots, \overline{v}_d) < \frac{\sqrt{3}}{2} D(v_1, \ldots, v_d).$$

Suppose now that iterating Step 2 never produces a reduced basis. Then, eventually, $D(v_1,\dots,v_d)$ must contradict the lower bound provided by Lemma 7.7 and we conclude that there are only finitely many iteration of Step 2 possible.

Remark 7.9.
The analysis of the proof can be refined to show that the running time of the LLL-algorithm is polynomial in the dimension d and the input size of the lattice Λ.

To end this section, we show that every reduced basis $\{v_1,\dots,v_d\}$ of Λ satisfies the condition $\prod_{i\in[d]}\|v_i\| \le M\cdot\det(\Lambda)$ were the constant M can be chosen as $M=2^{\frac{d(d-1)}{2}}$. We first prove the following useful lemma.

Lemma 7.10.
Let $\mathcal{B}=\{v_1,\dots,v_d\}$ be a weakly reduced basis for $\Lambda\subset\mathbb{R}^d$ with associated Gram-Schmidt-orthogonolization $\mathcal{B}_{GS}=\{w_1,\dots,w_d\}$. Then

$$\|w_j\|^2 \le \|v_j\|^2 \le \|w_j\|^2 + \frac{1}{4}\sum_{k\in[j-1]}\|w_k\|^2$$

for all $j\in[d]$.

Moreover, if $\mathcal{B}$ is a reduced basis then $\frac{1}{2}\|w_j\|^2\le\|w_{j+1}\|^2$ for all $j\in[d-1]$.

Proof. The assumption that $\mathcal{B}=\{v_1,\dots,v_d\}$ is a weakly reduced basis implies that

$$v_j = w_j + \sum_{\ell\in[j-1]}\lambda_{j\ell}w_\ell$$

where $|\lambda_{j\ell}|\le\frac{1}{2}$. The first claim follows since $\{w_1,\dots,w_d\}$ consists of pairwise orthogonal vectors:

$$\|v_j\|^2 = \|w_j\|^2 + \sum_{k\in[j-1]}\|\lambda_{jk}w_k\|^2.$$

For the second claim, we first remark that $\{w_1,\dots,w_d\}$ is pairwise orthogonal and compatible to the flag $V_0,V_1,\dots,V_d$. In particular, we have

$$\mathsf{dist}(v_j,V_{j-1})^2 = \|w_j\|^2 \qquad\text{and}\qquad \mathsf{dist}(v_{j+1},V_{j-1})^2 = \|w_{j+1}\|^2 + \|\lambda_{j+1,j}w_j\|^2.$$

Moreover, as $\mathcal{B}=\{v_1,\dots,v_d\}$ is a reduced basis by assumption, we have

$$\frac{3}{4}\cdot\mathsf{dist}(v_j,V_{j-1})^2 \le \mathsf{dist}(v_{j+1},V_{j-1})^2.$$

If we combine these properties, we obtain

$$\frac{3}{4}\|w_k\|^2 \le \|w_{k+1}\|^2 + \|\lambda_{k+1,k}w_k\|^2 = \|w_{k+1}\|^2 + \frac{1}{4}\|w_k\|^2$$

and the second claim follows. □

Corollary 7.11.
If $\mathcal{B}=\{v_1,\dots,v_d\}$ is a reduced basis of $\Lambda\subset\mathbb{R}^d$ then

$$\prod_{i\in[d]}\|v_i\| \le 2^{\frac{d(d-1)}{2}}\det(\Lambda).$$

Proof. Since $\mathcal{B}$ is a reduced basis, we have

$$\|v_j\|^2 \le \|w_j\|^2 + \frac{1}{4}\sum_{k=1}^{j-1}2^{j-k}\|w_j\|^2 = \Big(1+\frac{1}{2}\sum_{k=0}^{j-2}2^k\Big)\|w_j\|^2 \le \Big(1+\sum_{k=0}^{j-2}2^k\Big)\|w_j\|^2 = 2^{j-1}\|w_j\|^2.$$

This implies

$$\prod_{i\in[d]}\|v_i\| \le \prod_{i\in[d]}2^{i-1}\|w_i\|^2 = 2^{\frac{d(d-1)}{2}}\det(\Lambda).$$

□

8. Geometry of numbers

8.1. Minkowski's Convex body Theorems.

We prove Minkowski's First and Second Convex Body Theorems. Throughout this section, we assume that $\Lambda \subset \mathbb{R}^d$ is a lattice of rank d.

Definition 8.1 (convex body, centrally symmetric set)**.**
i) A convex body $K \subset \mathbb{R}^d$ is a compact convex set with nonempty interior.
ii) A set $C \subset \mathbb{R}^d$ is centrally symmetric if $x \in C$ implies $= x \in C$.

Theorem 8.2 (Blichfeldt, 1914)**.**
If $S \subset \mathbb{R}^d$ is a set with $\mathsf{vol}_{\mathbb{R}^d}(S) > \det(\Lambda)$ then there are $p, q \in S$ such that

$$p - q \in \Lambda \setminus \{0\}.$$

Proof. If $\Pi = \Pi_\Lambda$ is a fundamental parallelepiped of Λ then $\mathsf{vol}_{\mathbb{R}^d}(\Pi) = \det(\Lambda) < \mathsf{vol}_{\mathbb{R}^d}(S)$. We define

$$S_x := \{y \in \Pi \mid x + y \in S\}$$

for all $x \in \Lambda$. Notice that S is covered without overlap by the sets $(x + \Pi) \cap S$ for $x \in \Lambda$ and that $S_x = (x + \Pi) \cap S$ for all $x \in \Lambda$. This implies

$$\mathsf{vol}_{\mathbb{R}^d}(S) = \sum_{x \in \Lambda} \mathsf{vol}_{\mathbb{R}^d}((x + \Pi) \cap S) = \sum_{x \in \Lambda} \mathsf{vol}_{\mathbb{R}^d}(S_x).$$

We now claim that $S_x \cap S_y \neq \varnothing$ for some distinct $x, y \in \Lambda$. To prove this, we suppose that $S_x \cap S_y = \varnothing$ for all $x, y \in \Lambda$ with $x \neq y$. Thus, we have

$$\mathsf{vol}_{\mathbb{R}^d}\Big(\bigcup_{x \in \Lambda} S_x\Big) = \sum_{x \in \Lambda} \mathsf{vol}_{\mathbb{R}^d}(S_x) = \mathsf{vol}_{\mathbb{R}^d}(S) > \mathsf{vol}_{\mathbb{R}^d}(\Pi)$$

which contradicts $\bigcup_{x \in \Lambda} S_x \subseteq \Pi$ and we find $x_0, y_0 \in \Lambda$ with $x_0 \neq y_0$ such that $S_{x_0} \cap S_{y_0} \neq \varnothing$. Now choose $a \in S_{x_0} \cap S_{y_0}$ and set

$$p := a + x_0 \in S \qquad \text{and} \qquad q := a + y_0 \in S.$$

This implies the claim $p - q = x_0 - y_0 \in \Lambda \setminus \{0\}$. □

Theorem 8.3 (Minkowski's First Convex Body Theorem, 1896)**.**
Let $S \subset \mathbb{R}^d$ be a centrally symmetric convex set with $\mathsf{vol}_{\mathbb{R}^d}(S) > 2^d \det(\Lambda)$. Then

$$(S \cap \Lambda) \setminus \{0\} \neq \varnothing.$$

Moreover, if S is compact then $\mathsf{vol}_{\mathbb{R}^d}(S) \geq 2^d \det(\Lambda)$ implies $(S \cap \Lambda) \setminus \{0\} \neq \varnothing$.

Proof. Consider the dilate $T := \frac{1}{2}S$. Then

$$\mathsf{vol}_{\mathbb{R}^d}(T) = 2^{-d}\mathsf{vol}_{\mathbb{R}^d}(S) > \det(\Lambda)$$

and Blichfeldt's Theorem (Theorem 8.2) guarantees that there exist $p, q \in S$ such that

$$x := \frac{1}{2}p - \frac{1}{2}q \in \Lambda \setminus \{0\}.$$

As S is centrally symmetric, we conclude that $-q \in S$ and $x \in S$ follows by convexity of S.

Assume now that the centrally symmetric convex set S is compact with $\mathsf{vol}_{\mathbb{R}^d}(S) = 2^d \det(\Lambda)$. For every $k \in \mathbb{N}$, we have $\mathsf{vol}_{\mathbb{R}^d}(\frac{k+1}{k}S) > 2^d \det(\Lambda)$ and, by the first part, there exists

$$x_k \in \left(\frac{k+1}{k}S \cap \Lambda\right) \setminus \{0\} \text{ for each } k \in \mathbb{N}$$

and $x_1, x_2, \ldots$ is a sequence of points $x_k \in \Lambda \setminus \{0\}$ with $x_k \in \frac{k+1}{k}S \subset 2S$. Now $2S$ is compact, so we obtain a convergent subsequence $(x_{k_i})_{i \in \mathbb{N}}$ and, as Λ is discrete, there exists $N \in \mathbb{N}$ such that $x_{k_i} = x$ for all $i \geq N$ and $x = x_{k_N}$. Now $x \in \Lambda \setminus \{0\}$ and $x = \lim_{i \to \infty} \frac{k}{k_1} x_{k_i} \in K$. □

Remark 8.4.
i) A centrally symmetric convex body $K \subset \mathbb{R}^d$ with $\mathsf{vol}_{\mathbb{R}^d}(K) = s^d \det \Lambda$ is called *extremal body* if $K \cap \Lambda = \{0\}$.

ii) Minkowski's First Convex Body Theorem only guarantees that there exists a point $x \in (S \cap \Lambda) \setminus \{0\}$, the proof is not constructive. Nevertheless, such a point can be constructed if we use additional tools such as the Theorem of Lenstra, Lenstra and Lovász.

Definition 8.5 (successive minima)**.**
For $k \in [d]$, the k^{th} successive minimum λ_k of a centrally symmetric convex body $S \subset \mathbb{R}^d$ is defined as

$$\lambda_k := \inf \{\lambda > 0 \mid \dim(\mathsf{span}_{\mathbb{R}} \lambda S \cap \Lambda) \geq k\}.$$

Remark 8.6.
As Λ is a discrete set, conclude that the firrst successive minimum satisfies $\lambda_1 > 0$. Moreover, the definition of successive minima Â´implies $\lambda_1 \leq \lambda_2 \leq \ldots \leq \lambda_d$.

Lemma 8.7.
The first successive minimum of a centrally symmetric convex body $S \subset \mathbb{R}^d$ satisfies

$$\lambda_1^d \mathsf{vol}_{\mathbb{R}^d}(S) \leq 2^d \det(\Lambda).$$

Lemma 8.7 is easily proved and has the following improvement. We do not prove this generalized statement.

Theorem 8.8 (Minkowski's Second Convex Body Theorem, 1896)**.**
If $S \subset \mathbb{R}^d$ is a centrally symmetric convex body then its successive minima satify

$$\frac{2^d}{d!} \det(\Lambda) \leq \mathsf{vol}_{\mathbb{R}^d}(S) \prod_{k \in [d]} \lambda_k \leq 2^d \det(\Lambda).$$

Blichfeldt's Theorem and Minkowski's First Convex Body Theorem have the following straightforward generalizations.

Theorem 8.9 (Generalized Blichfeldt's Theorem)**.**
Let $S \subset \mathbb{R}^d$ be a Lebesgue-measurable set with $m \det(\Lambda) \leq \mathsf{vol}_{\mathbb{R}^d}(S)$ for some $m \in \mathbb{N}$. Then there exist $m+1$ points $p_1, \ldots, p_{m+1} \in S$ such that $p_i - p_j \in \Lambda \setminus \{0\}$ for all distinct chosices $i, j \in [m+1]$.

Proof. Without loss of generality, we assume that S is bounded since we clearly restrict to bounded subset $S' \subset S$ that satisfies $m \det(\Lambda) \leq \mathsf{vol}_{\mathbb{R}^d}(S')$ otherwise.

As in the proof of Blichfeldt's Theorem (Theorem 8.2), we choose a fundamental parallelepied Π of Λ and define $S_x := \{y \in \Pi \mid x + y \in S\}$ for all $x \in \Lambda$. Furthermore, we consider the indicator function of S_x:

$$\mathbb{1}_x : \mathbb{R}^d \longrightarrow \mathbb{Z} \qquad \text{via} \qquad z \longmapsto \begin{cases} 0 & z \notin S_x; \\ 1 & z \in S_x; \end{cases}$$

and set $f := \sum_{x \in \Lambda} \mathbb{1}_x$. Notice that the sum in the definition of f is a finite sum since Π and S are bounded sets. Then

$$\int_\Pi f(x)dx = \sum_{y \in \Lambda} \int_\Pi \mathbb{1}_y dx = \sum_{y \in \Lambda} \mathsf{vol}_{\mathbb{R}^d}(S_y) = \sum_{y \in \Lambda} \mathsf{vol}_{\mathbb{R}^d}((\Pi + y) \cap S) = \mathsf{vol}_{\mathbb{R}^d}(S).$$

Now $\int_\Pi \mathbb{1} dx = \det(\Lambda)$ implies the existence of $y \in \Pi$ such that $f(y) > m$. More precisely, $f(y) \geq m + 1$ as $f : \mathbb{R}^d \longrightarrow \mathbb{Z}$. But this implies the existence of pairwise distinct points $x_1, \ldots, x_{m+1} \in \Lambda$ such that $y \in \bigcap_{i \in [m+1]} \S_{x_i}$ and we define

$$p_i := y + x_i \in S \qquad \text{for } i \in [m+1]$$

to obtain the desired points. □

Theorem 8.10 (van der Corputh, 1935)**.**
If $S \subset \mathbb{R}^d$ is a centrally symmetric convex set with $m \cdot 2^d \det(\Lambda) < \mathsf{vol}_{\mathbb{R}^d}(S)$ for some $m \in \mathbb{N}$ then there exist m pairwise distinct pairs $\pm x_1, \ldots, \pm x_m \in (S \cap \Lambda) \setminus \{0\}$.

Proof. If we consider the dilate $T := \frac{1}{2}S$ then

$$m \det(\Lambda) < \frac{1}{2^d}\mathsf{vol}_{\mathbb{R}^d}(S) = \mathsf{vol}_{\mathbb{R}^d}(T)$$

and we can apply the generalized Blichfeldt's Theorem (Theorem 8.9) to obtain $m+1$ points $p_1, \ldots, p_{m+1} \in T$ such that $p_i - p_j \in \Lambda \setminus \{0\}$ for all $i, j \in [m+1]$ with $i \neq j$. If we define

$$x_i := p_i - p_{m+1} \qquad \text{for all } i \in [m]$$

then $x_i \in S$ since $p_j \in T = \frac{1}{2}S$ for all $j \in [m+1]$ and $S = T + T$. □

Corollary 8.11.
If $S \subset \mathbb{R}^d$ is a centrally symmetric convex set then

$$\mathsf{vol}_{\mathbb{R}^d}(S) \leq 2^{d-1}\left(\left|\mathrm{int}(S) \cap \mathbb{Z}^d\right| + 1\right).$$

Theorem 8.12 (Minkowski, 1910)**.**
If $S \subset \mathbb{R}^d$ is centrally symmetric and convex with $\mathrm{int}(S) \cap \Lambda = \{0\}$ *then*

$$|S \cap \Lambda| \leq 3^d.$$

Since the general case is obtained from the special case $\Lambda = \mathbb{Z}^d$ by an obvious lattice transformation, we prove Theorem 8.12 only in the situation $\Lambda = \mathbb{Z}^d$.

Proof. We aim for a contradiction and suppose that $|S \cap \Lambda| > 3^d$. As key ingredient of the proof, we consider the following homomorphism of groups:

$$\varphi : \mathbb{Z}^d \longrightarrow (\mathbb{Z}/3\mathbb{Z})^d \qquad \text{defined via} \qquad \begin{pmatrix} x_1 \\ \vdots \\ x_d \end{pmatrix} \longmapsto \begin{pmatrix} x_1 \pmod 3 \\ \vdots \\ x_d \pmod 3 \end{pmatrix}.$$

We notice that $\left|(\mathbb{Z}/3\mathbb{Z})^d\right| = 3^d$ and obtain distinct $x, y \in S \cap \mathbb{Z}^d$ such that $\varphi(x) = \varphi(y)$ by the pigeonhole principle. Thus $\varphi(x-y) = 0$ and we have $\frac{x-y}{3} \in \mathbb{Z}^d$. The central symmetry of S implies $-y \in S$ and we obtain

$$0 \neq p = \frac{x}{3} + \frac{-y}{3} \in \frac{2}{3}S.$$

This clearly contradicts $\mathrm{int}(S) \cap \Lambda = \{0\}$. □

Remark 8.13. Up to unimodular transformations, the d-dimensional standard cube $[-1;1]^d$ is the only centrally symmetric lattice polytope P with $\mathrm{int}(P) \cap \mathbb{Z}^d = \{0\}$ and $\left|p \cap \mathbb{Z}^d\right| = 3^d$. This is a result of Draisma, McAllister & Nill (2009).

8.2. **Lagrange's Theorem.**
This section applies Minkowski's First Convex Body Theorem to number theory. We prove a classic result that every positive integer is the sum of four squares of integers!

Lemma 8.14.
For $m \in \mathbb{N}$, let $c_1, \ldots, c_m \in \mathbb{Z}^d$, $\gamma_1, \ldots, \gamma_m \in \mathbb{N}$ and define

$$\Lambda := \left\{x \in \mathbb{Z}^d \;\middle|\; \langle c_i, x\rangle \equiv 0 \pmod{\gamma_i} \text{ for all } i \in [m]\right\}.$$

Then Λ is a lattice of rank d and $\det(\Lambda) \leq \gamma_1 \cdot \ldots \cdot \gamma_m$.

Proof. Clearly, Λ is a discrete subgroup of $\mathbb{R}^d$, so Λ is a lattice and we have to determine its rank. If we write $\gamma := \gamma_1 \cdot \ldots \cdot \gamma_m \in \mathbb{N}$ then $\gamma\mathbb{Z}^d \subset \mathbb{Z}^d$ and $z \in \Lambda$ for all $z \in \gamma\mathbb{Z}^d$ are immediate. This proves $\mathsf{rk}(\Lambda) = d$.

We now prove the upper bound for $\det(\Lambda)$. Using Corollary 2.15 and Corollary 2.13, we have

$$\det(\Lambda) = \det(M_{\mathcal{B}_\Lambda}) = |\Pi_{\mathcal{B}_\Lambda}| = \left|\mathbb{Z}^d/\Lambda\right|$$

and, instead of $\det(\Lambda)$, we bound the number of cosets of $\mathbb{Z}^d/\Lambda$. First, define $\mathcal{R} \subset \mathbb{Z}^m$ via

$$r \in \mathcal{R} \qquad \Longleftrightarrow \qquad r := \begin{pmatrix} r_1 \\ \vdots \\ r_m \end{pmatrix} \quad \text{where } 0 \leq r_i < \gamma_i \text{ for all } i \in [m].$$

Second, whenever possible, choose $x_r \in \mathbb{Z}^d$ for $r \in \mathcal{R}$ such that

$$\langle c_i, x_r \rangle \equiv r_i \pmod{\gamma_i} \qquad \text{for all } i \in [m].$$

In particular, $x_{\mathbf{0}} \in \Lambda$ and for every $x \in \mathbb{Z}^d$ there is a unique $r \in \mathcal{R}$ such that

$$\langle c_i, x \rangle \equiv \langle c_i, x_r \rangle \equiv r_i \pmod{\gamma_i} \qquad \text{for all } i \in [m].$$

This shows that $\mathbb{Z}^d/\Lambda$ consists of at most $|\mathcal{R}| = \gamma$ cosets. □

Theorem 8.15 (Lagrange's Theorem)**.**
For every $n \in \mathbb{N}$ there exist $a, b, c, d \in \mathbb{Z}$ such that $a^2 + b^2 + c^2 + d^2 = n$.

Proof. The proof proceeds in four steps.

Step 1: For all $a_1, a_2, b_1, b_2, c_1, c_2, d_1, d_2 \in \mathbb{Z}$ there exist $a, b, c, d \in \mathbb{Z}$ such that

$$\left(a_1^2 + b_1^2 + c_1^2 + d_1^2\right)\left(a_2^2 + b_2^2 + c_2^2 + d_2^2\right) = a^2 + b^2 + c^2 + d^2.$$

Proof. Exercise. □

Step 2: Every $n \in \mathbb{N}$ is the product of primes, so Lagrange's Theorem for all primes suffices.

Step 3: For every prime p there exist $a, b \in \mathbb{Z}$ such that $a^2 + b^2 + 1 \equiv 0 \pmod{n}$.

Proof. The claim is trivial if $p = 2$ (set $a = 1$ and $b = 0$), so let p be an odd prime.

We claim that $0 \le a < \frac{p}{2}$ yields $\frac{p+1}{2}$ pairwise distinct residues $a^2 \pmod{p}$ as well as $\frac{p+1}{2}$ pairwise distinct residues $-1 - a^2 \pmod{p}$.

We prove the claim for the residues $a^2 \pmod{p}$. If $0 \le \lambda, \mu < \frac{p}{2}$ with $\lambda \neq \mu$ then

$$\lambda - \mu \not\equiv 0 \pmod{p} \qquad \text{and} \qquad \lambda + \mu \not\equiv 0 \pmod{p}.$$

Since p is a prime, we have $(\lambda + \mu)(\lambda - \mu) \not\equiv 0 \pmod{p}$. This proves $\lambda^2 \not\equiv \mu^2 \pmod{p}$.

Both claims imply

$$a^2 \equiv -1 - b^2 \pmod{p} \qquad \text{for some } 0 \le a, b < \frac{p}{2}$$

and this choice yields

$$a^2 + b^2 + 1 \equiv 0 \pmod{p}.$$

□

Step 4: We now use the lattice of Lemma 8.14 that encoded number theory.

If we define

$$\Lambda := \left\{ \begin{pmatrix} w \\ x \\ y \\ z \end{pmatrix} \in \mathbb{Z}^4 \;\middle|\; \begin{array}{c} \langle \begin{pmatrix} 1 \\ 0 \\ -a \\ -b \end{pmatrix}, \begin{pmatrix} w \\ x \\ y \\ z \end{pmatrix} \rangle \equiv 0 \pmod{p} \\ \text{and} \\ \langle \begin{pmatrix} 0 \\ 1 \\ -b \\ a \end{pmatrix}, \begin{pmatrix} w \\ x \\ y \\ z \end{pmatrix} \rangle \equiv 0 \pmod{p} \end{array} \right\}$$

then Lemma 8.14 implies that Λ is a lattice with $\mathsf{rk}(\Lambda) = 4$ and $\det(\Lambda) = |\mathbb{Z}^4/\Lambda| \le p^2$.

We consider the open ball

$$B_{\sqrt{2p}} := \left\{ v \in \mathbb{R}^4 \;\middle|\; \|v\| < \sqrt{2p} \right\}$$

and estimate its volume as

$$\mathsf{vol}_{\mathbb{R}^d}(B_{\sqrt{2p}}) = 2p^2\pi^2 > 16p^2 \ge 2^4 \det(\Lambda).$$

Now Minkowski's First Convex Body Theorem (Theorem 8.3) implies the existence of $u \in (B_{\sqrt{2p}} \cap \Lambda) \setminus \{0\}$. Then $u \in B_{\sqrt{2p}}$ yields

$$0 < u_1^2 + u_2^2 + u_3^2 + u_4^2 < 2p$$

and $u \in \Lambda$ implies

$$u_1^2 + u_2^2 + u_3^2 + u_4^2 \equiv \left(a^2 + b^2 + 1\right) u_3^2 + \left(a^2 + b^2 + 1\right) u_4^2 \equiv 0 \pmod{p}.$$

This shows that $\|u\|^2$ is divisible by p and $0 < \|u\|^2 < 2p$ implies $\|u\|^2 = p$. □

8.3. **Packing and covering radii of lattices and flatness theorems.**
The aim of this section is to prove that a convex body $S \subset \mathbb{R}^d$ with $S \cap \Lambda = \varnothing$ cannot be 'thick' in all directions (we give a precise definition of thickness in Defintion **??**). The proof relies on the the relation of the lattice Λ and its dual lattice Λ^*. In particular, we use estimates that involve certain lattice invariants ('packing radius' and 'covering radius').

Remark 8.16 (dual lattices and euclidean vector spaces)**.**
We briefly recall some views on dual lattices and emphasize differences if a lattice Λ of rank d is embedded in an abstract $\mathbb{R}$-vector space V of dimension d or in a euclidean vector space, that is, some $\mathbb{R}$-vector space V together with a positive bilinaer form $b(\ ,\ )$. Of course, V may be replaced by $\mathbb{R}^d$ and the general euclidean vector space may be replaced by $\mathbb{R}^d$ together with the standard inner product $\langle\ ,\ \rangle$.

algebraic view: If a lattice $\Lambda \subset V$ is given via $\mathsf{span}_{\mathbb{Z}}(v_1, \ldots, v_d)$ by a lattice basis $\{v_1, \ldots, v_d\}$ then V can be algebraically recovered (up to an isomorphism) using tensor products: $V \cong \Lambda \otimes_{\mathbb{Z}} \mathbb{R}$. In general, the dual vector space V^* is defined as the vector space $Hom_{\mathbb{R}}(V, \mathbb{R})$ of all $\mathbb{R}$-linear maps $f : V \longrightarrow \mathbb{R}$. This abstract point of view emphasizes $V \neq V^*$ and $\Lambda \otimes_{\mathbb{Z}} \mathbb{R} \neq (\Lambda \otimes_{\mathbb{Z}} \mathbb{R})^*$. It is not difficult to check that the set $\Lambda^* := Hom_{\mathbb{Z}}(\Lambda, \mathbb{Z})$ of all $\mathbb{Z}$-linear maps $f : \Lambda \longrightarrow \mathbb{Z}$ is actually a lattice $\Lambda^* \subset (\Lambda \otimes_{\mathbb{Z}} \mathbb{R})^*$ and we have

$$\Lambda^* \subset (\Lambda \otimes_{\mathbb{Z}} \mathbb{R})^* = Hom_{\mathbb{R}}(\Lambda \otimes_{\mathbb{Z}} \mathbb{R}, \mathbb{R}) \cong Hom_{\mathbb{R}}(V, \mathbb{R}) = V^*,$$

because of the identification $V \cong \Lambda \otimes_{\mathbb{Z}} \mathbb{R}$. This justifies the abuse of notation to write statements like 'let $\Lambda^* \subset V^*$ be a lattice'.

geometric view: The most frequent use of the bilinear form $b(\ ,\ )$ of a euclidean vector space V is probably to measure geometric quantities such as lengths and angles. Beyond this geometric motivation, the bilinear form provides a canonical isomorphism $\varphi : V \longrightarrow V^*$ via $\varphi(v) := b(v,\ )$ if $\dim(V) < \infty$. Using this isomorphism we can identify $\Lambda^* \subset V^*$ with a lattice $\widetilde{\Lambda} \subset V$ (which is distinct from Λ most of the time) and this identification justifies the common abuse of notation $\Lambda^* \subset V$. This identification is the source of interesting questions such as the classification of self-dual lattices $\Lambda = \Lambda^*$ but it can also be the source of painful ambiguities or mistakes.

Technische Universität München, Zentrum Mathematik.
E-mail address: lange@ma.tum.de